Analysis of Identification Systems Adoption in Selected African Countries

Adjei, Joseph K.

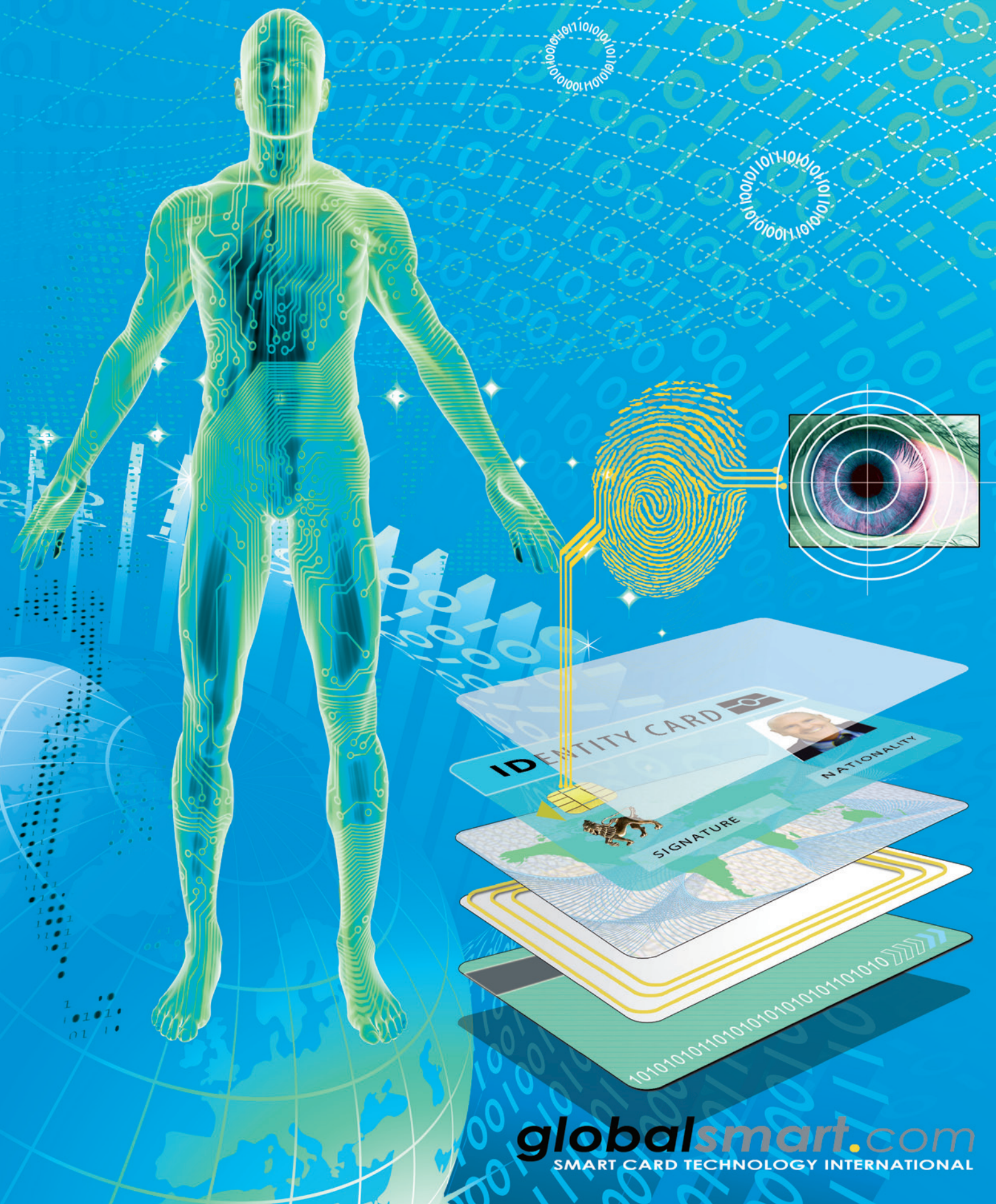
Published in:
ID Credentials

Publication date:
2011

Document Version
Early version, also known as pre-print

ID CREDENTIALS

Secure Identity Solutions



globalsmart.com

SMART CARD TECHNOLOGY INTERNATIONAL

MÜHLBAUER GROUP

Providing new perspectives in smart document solutions

We live identification! For 30 years the Mühlbauer Group has been a premium partner for private companies and the public sector in the areas of plastic and chip cards, passports and various RFID applications around the world.

Our unique product portfolio affords us the position to be the preferred technology partner for governments, security printers and system integrators. Precision down to the smallest detail, highest flexibility, absolute reliability and a full commitment are our plenary premises. Our open interfaces and the easy integration of our systems give us quick reaction to our client's requirements.

We provide complete support to our client's in the selection, development and implementation of their individual solution. Not surprisingly the world trusts Mühlbauer for complex projects in the security sectors of ID cards and ePassports.

Trust in the smart ID specialist – trust in Mühlbauer.

Mühlbauer
High Tech International

The One-Stop Partner for Turnkey Solutions

- Project consulting, planning & realization
- Logical & physical infrastructure and security
- Application development
- Data enrollment, management & security solutions
- Production, personalization & mailing solutions
- Surface and stand-alone print inspection systems
- Border control & verification solutions
- Technology & know-how transfer

Mühlbauer AG
Josef-Mühlbauer-Platz 1
D-93426 Roding
tel. +49-9461-952-0
fax. +49-9461-952-1101
www.muehlbauer.de

Australia | Brazil | China | France | Germany | India | Malaysia | Mexico | Russia | Serbia
Slovakia | South Africa | South Korea | Taiwan | Turkey | Uganda | United Arabian Emirates | U.S.A.

BRING YOUR SECURE ID PROGRAM INTO FOCUS

HIGHER SECURITY. GREATER EFFICIENCY. LOWER RISK.

Datacard Group solves complex identity issues for governments worldwide. We combine a deep understanding of industry best practices and standards with our secure identity solutions—which include best-in-class personalization, identity management software, supplies and service—to deliver highly secure identity documents. In collaboration with integrator partners and governments, we help plan and implement identification programs that improve security, maximize efficiency and help reduce risk for governments.

Governments in more than 90 countries have trusted Datacard® solutions for over 350 programs, including national IDs, travel documents, driver's licenses, healthcare and e-government applications.

To learn more, visit datacard.com/government

DatacardGroup

Contents

Secure identification systems from Giesecke & Devrient

Creating Confidence. G&D is a leading company in smart chip-based solutions for secure ID documents and passports, and boasts in-depth experience in the field of high-security documents. We supply entire nations with passport and border control systems, ID card solutions and have become a trusted adviser and supplier to governments. We also provide customized document features, card operating systems and technology for integrating state-of-the-art security features into ID documents. G&D will find the best solution for your individual needs. We define requirements together with you and offer tailor-made, effectively protected products that meet international standards. ID system implementation by G&D – individual, international and secure. **www.gi-de.com**

Giesecke & Devrient

Creating Confidence.

Contents

Advertisers

Gold hologram corporate logo courtesy of:

Applied Optical Technologies

Credits

EDITOR	Wendy Atkins
SUB EDITOR	Liz Harrison
PUBLISHER	Tim Courtney
PRODUCTION MANAGER	Jo O'Connor
PRINTED & BOUND	Ian Allan Printing Ltd.
DISTRIBUTION	globalsmart.com

Smart Card Technology International
ID CREDENTIALS

134 Lots Road, Chelsea,
London SW10 ORJ, UK
Tel: +44 (0)20 7385 8811
Email: info@globalsmart.com
Web: www.globalsmart.com

Worldwide book sales & subscriptions:
Chancery Hurst Books

Registered with the British Library ISSN 1361 8288

Oberthur Technologies

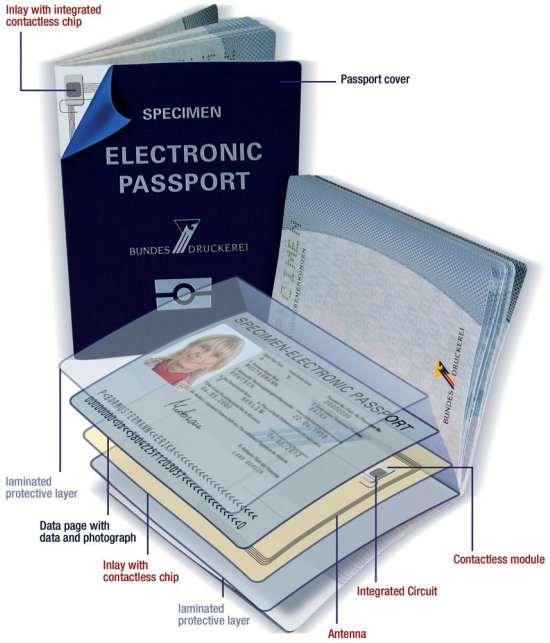
Security solutions for a changing world

Oberthur Technologies is a world leader in the field of secure technologies. Innovation and excellence ensure Oberthur Technologies' strong positioning in its main target markets:

- Card Systems: World's second largest provider of security and identification solutions and services based on smart card technologies for mobile, payment, transport, digital TV and convergence markets.
- Identity: A world leader in the manufacture of traditional and electronic secure identity documents. We are also a system integrator and a specialist in know-how transfer – census, personalization platforms implementation and identity data management.
- Security printing: World's third largest private security printer specialized in the production of banknotes, checks and numerous security documents in more than fifty countries.
- Cash protection: World leader in design and manufacture of intelligent cash protection solutions for CIT (Cash In Transit) companies, ATM manufacturers and owners, retailers, post offices and banks.

Close to its customers, Oberthur Technologies benefits from an industrial and commercial presence across all five continents.

www.oberthur.com



Source: Bundesdruckerei GmbH

"The Global ePassport and eVisa Industry Report" : Figures for 2009-2014

Some figures have been released from a report by Acuity, "The Global ePassport and eVisa Industry Report", that show that the market is burgeoning, and when taken together will produce $11 billion in annual revenue by 2014. A selection of figures from the report can be broken down as follows:

ePassport

In 2009, the ePassport accounted for 73% of the revenue market share, which will drop to 67% by 2014, but in terms of volume of issued passports, it grows from 61 million to 130 million in the same period. Its revenue market share goes down from 73% in 2009 to 67% by 2014.

Europe currently dominates the market, taking a 53% share, but this dominance shifts to Asia, whose share increases from 17% to 35% while Europe's drops to 35%. By 2014, the top ten ePassport issuing countries (in order of rank: India, US, China, Brazil, UK, Philippines, Japan, France, Canada, Indonesia) will account for 59% of the market of ePassport issuing volume, (77 million documents) and 58% of global market revenue ($2.7 billion).

With a CAGR of 25.28% from 2009 to 2014, the market will reach sustainable annual revenues in excess of $7 billion by 2014, with the strongest growth coming from South America.

eVisa

The eVisa's growth in issuance increases from around 14 million to 61 million, and the number of countries which issue them grows from 9 to 66, which will comprise almost 90% of annually issued visas globally from 2009 till 2014.

The top 10 eVisa issuing countries (in order of rank: China, Australia, US, UK, Canada, Germany, France, Russia, Italy, Finland) will have produced 56 million documents representing 93% of the total volume, bringing $2.6 billion in revenue, which amounts to 73% of the global eVisa issuance revenue, by 2014.

The eVisa market has a CAGR of 32.84%, including both hard and software, plus services related to the development and implementation of eVisa programs, during that same period.

A Sustainable Market

The ongoing development and production of a secure infrastructure, the stabilisation of existing programs, the continuous incorporation of security features, the updating and replacing of aging equipment and the re-issuing of documents in 5 to 10 year cycles, will provide sustainable market opportunities in the ePassport and eVisa industry.

The Global Need for Effective Border Control

These days, fear of terrorism, anger at illegal immigration and worry about identity theft have resulted in security issues being taken in hand. A major area of concern has been how to implement effective control at borders, thus governments and organisations such as the International Civil Aviation Authority (ICAO) have been working to increase security for international travel and the safeguarding of personal data.

The ICAO has worked towards establishing an internationally common standard for the reading of travel documents and the use of passport data, and as of April 2010, all ICAO contracted states have to have issued either machine readable passports, or ePassports that can hold encrypted biometric data.

Although about 170 contracted countries have already complied with issuing the new passports, some as early as 2004, not all countries, as yet, have the necessary infrastructure to read and verify the information contained in them. However, all major airports have been working towards creating appropriate e-border controls throughout 2010.

Source: Assa Abloy Identification Technologies- Aontec

Interpol to Use High Security Multi Purpose Credentials

ENTRUST has collaborated with EDAPS consortium (which leads a grouping of 20 suppliers from 12 countries), to provide Interpol with eID cards and ePassports that provide the highest security credentials for Interpol staff and law enforcement officers.

These ICAO compliant credentials will enable officers, from any of its 188 National Central Bureaux, to identify themselves at international borders as well as cross them quickly when on Interpol related business, such as responding to serious crime or disasters, or when participating in official events. So far, while criminals have been able to move quickly and effortlessly across borders, Interpol officials have been slowed down or stopped by bureaucratic, international red tape.

They will also be able to identify themselves at Interpol's General Secretariat or any other Interpol facility, as well as to communicate securely from virtually any fixed or mobile location in the world. Ronald K Noble, Interpol Secretary General said, "As deliberate attacks on government and enterprise entities continue to grow in number and sophistication, proper identity-based security needs to be applied".

Bill Connor, Entrust's president and CEO, says, "These credentials can be tailored for any environment whether the need is for electronic machine readable travel documents (eMRTD) or more advanced BAC and EAC ePassports".

The travel documents gained approval from Interpol's Executive Committee in March 2009, and were first presented to member countries at the Interpol General Assembly in November 2009. According to Entrust, Brazil has already examined the security features of both documents and determined that they meet high-level security standards, and numerous other countries either have granted the new e-documents recognition or are in the process of evaluating their future recognition.

US Bill to Introduce Biometric ID Card

The US government has proposed a national ID card with a difference. It is designed to combat the employment of undocumented workers or illegal immigrants. They have called it a `biometric social security card' because it will only be seen by employers as an electronic verification of the holders eligibility to work, and cannot be used as a means of identification in any other circumstances.

To quote from the bill, it will be in the form of a "fraud - resistant, tamper-resistant, wear- resistant, machine-readable social security card containing a photograph and an electronically coded micro-processing chip which possesses a unique biometric identifier for the authorised card bearer"

Brief Analysis of ID Card Usage in the EU

A questionnaire, designed to analyse the use of ID cards by the EU member states and members of the "Mixed Committee," came up with the following results:

Denmark, Finland, France, Greece, Ireland, Latvia and the Netherlands did not contribute. Of the 22 that did, only 17 have a mandatory ID card. Of the 17 that use them, 13 of them use traditional cards, and 8 use cards with contact or contactless chips that have the capacity to store biometric data. Of the 8 countries who could, only 7 have included biometric data.
The answers from the UK were not included because the new government scrapped the ID scheme.
This analysis was taken from a briefing by Statewatch.
For further information see http://www.statewatch.org/analyses/no-107-national-ID-cards-questionnaire.pdf

The Secure idenTity acrOss boRders linKed (STORK) Project Pilots.

The STORK project, which is a three-year initiative, aims at creating an EU-wide interoperable system for eID recognition and authentication that enables citizens, businesses and government employees to use their national electronic identities in any member state. It involves 17 EU countries and is supported by the European Commission and the ICT Policy Support Programme (ICT PSP), which aims at stimulating innovation and competitiveness through the wider uptake and best use of ICT by citizens, governments and businesses.

The project has been created to develop common rules and specifications to assist mutual recognition of eIDs across national borders, to test secure and easy-to-use eID solutions for businesses and citizens, and to interact with other EU initiatives to maximise the usefulness of eID services.
To this end, six STORK pilots have gone live, in which eleven European countries are participating:

1. Cross-border Authentication Platform for Electronic Services, which shows that cross-border electronic services can operate in several member states. This involves national portals from Austria (help.gv.at), Estonia (eesti.ee), Germany (mein-service-BW), Portugal (portaldocidadao.pt), one regional portal from Catalonia in Spain and one specific service for compliance activities for working in Belgium (limosa.be).
2. Safer Chat, which is to promote safety on the internet for children and young adults, particularly when meeting people online. It will also make things safer for all internet users, helping to prevent fraud and identity theft. A major objective of this pilot is to build a platform for a safer online environment where people can communicate online using their eIDs.
3. Student Mobility is to help students who want to study in Member States that are not their own. It is to facilitate

their mobility across Europe, and allow them to access any online administration service on offer from a particular University, using their eID card from the country of origin, either for e-identification or for e-signatures.

4. Cross-border eDelivery, which aims to create a basic framework enabling countries and their public administrations to send documents to citizens of different countries directly through the citizen's domestic eDelivery portal. EU citizens can live and work freely throughout the Union, and when living in a Member State that is not their country of origin, it is important that they can access online public services. The STORK interoperability layer enables participating citizens to use their eID to assert their identity and authenticate themselves.

5. Change of Address, which is to help EU citizens who wish to move or settle in another EU country. The interoperable service enables foreign citizens to notify all relevant parties involved without changing their own national eID credentials, and without having to change processes that are currently being used in each Member State.

6. Commission Services; the European Commission Authentication Service (ECAS) allows access to the numerous electronic services or support communication between Member States that require user authentication. The integration of STORK with ECAS has created the framework which allows the seamless integration of national eIDs.

The pilots, which started in the middle of 2010, are due to run for 12 months.

The EU Introduces Electronic Vehicle Registration Cards

An EU directive issued in 2003, allowing member countries to introduce electronic vehicle registration cards, eVRC's, to replace paper versions, became a subject for discussion over the next six years. By the end of 2009, transport ministries in member countries had become increasingly interested in it. Currently, Slovakia, the Netherlands and Austria are the only member states who are implementing it.

The card acts as a highly secure document, which simplifies vehicle checks both at home and abroad. The integrated microprocessor allows data to be read by a hand-held device more easily and reliably, which can then be sent, with the push of a button, to a central register for automated verification if needs be. It has to be compliant with ISO 7810 and smart card format ID-1. It must guarantee a service life of at least 10 years, and include at least 3 of the following safety features in its body: Microprinting; Iridescent printing; Guilloche printing; Laser engraving; UV ink; Optically variable ink (OVI); Inks with temperature-dependent colour; Holograms; Optically variable images; Variable laser images.

The idea is to create a security level that is comparable to the highly secure European ID cards, drivers' licenses and tachograph cards.

New Design for UK ePassport

The UK started issuing their new look ePassport in October, when De La Rue's 10 year, £400m contract for passport production began.

The latest security measures include:

- moving the chip which stores the holder's details to the inside of the passport cover where it will no longer be visible. This gives additional physical protection, as well as making it much harder to replace the chip without damage to the passport cover being spotted;
- a secondary image of the holder printed onto the observations page;
- a new transparent covering which includes several holograms to protect the holder's personal details; and
- new designs now stretching across two pages.

Pages of the passport contain images of famous landmarks from across the UK, such as the White Cliffs of Dover or the Giants Causeway, and the personal details have now been moved to the second page, bringing it in line with many other passports around the world. Biometric fingerprints, such as those used in EU passports, have not been included.

The new design is part of a strategy to help the UK stay ahead of those who fraudulently tamper with or copy passports.

Plans for the UK ID Card are Scrapped

In May, 2010 in a wave of priority legislation, the government announced that it was scrapping the UK ID card scheme, and destroying the National Identity Register which contains the biographic and biometric fingerprint data of card holders. The move will save around £86m and avoid ongoing costs of around £800m. The Deputy Prime Minister, Nick Clegg, said "...cancelling the scheme and abolishing the National Identity Register is a major step in dismantling the surveillance state..."

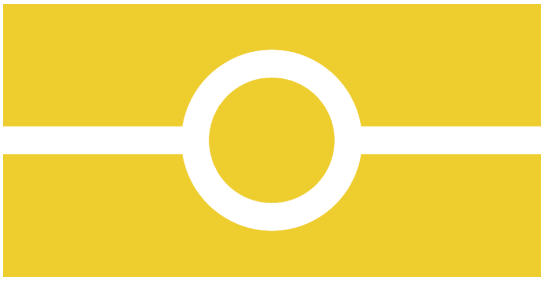
The New Multi-Functional German eID Card

On November 1st 2010, Germany started to replace citizens' old, expiring ID cards with the new eID card, a process which will take ten years. The new cards contain a microchip, NXP Semiconductors SmartMX secure contactless microcontroller chip, which uses Radio Frequency Identification (RFID)

technology. All the data that typically appears on the front of an ID card, such as a name, address, date of birth , hair and eye colour, place of issuance and a photo is still there but it is also contained within the micro chip along with a digital biometric photograph of the card holder. They also contain fingerprint scans and a six-digit PIN digital signature.

These features are designed to turn it into a very secure multifunctional card. It can now be used online for both e-government matters and for e-commerce, e.g. registering for online shopping on a home computer. There are security features in the card that protect against phishing sites, and a stronger encryption based on elliptic curve cryptography, which is thought to be essentially unbreakable. To use the online authentication function, a scanner is needed, and the government is going to distribute a million of them free as part of a 'stimulus package'.

Critics say that it is at this point that the system is most vulnerable. Card readers come in a variety of models and the Chaos Computer Club, a German hacker collective, publicly demonstrated that the most basic model could be circumvented using spyware. They say that this is really because many citizens do not understand how to manage the IT security on their systems. A spokesperson for CCC said "the hackers will always attack the weakest point and the weakest point is the user."



The Second Generation Italian Passport

Italy is issuing a second generation of ePassport, which will contain a digital facial image, a digital signature and two fingerprint images on the integrated RFID chip.

Italy-based biometrics vendor, Green Bit SpA, will supply the biometric enrolment solution. They are using their desktop Scan-Pass DTS_26, which is designed to allow for efficient and demographic data acquisition, as well as to create ease of use for people of any skill level. There should be 1,200 of the devices in place in all e-passport issuing offices around the country by the end of June 2011, ready for large-scale issuance before the start of the holiday season.

Poland's New eID Card

Poland is rolling out its new eID card from the beginning of 2011. It will have an electronic chip storing personal data, an electronic signature, which can be used as identification over the Internet, a digital facial image, and possibly some further biometric information. The card will be valid for ten years and, according to the findings of an ENISA survey, will probably be issued free of charge.

The budget for the project is anticipated to be in excess of US $130 million (€90.1 million) with US $110 (€76.2 million) of that sum being funded by the EU. In preparation for the issuance of the cards, the Polish Security Printing Works (the only security printing authority in Poland) has invested in the necessary infrastructure to support their use.

Bulgarian Biometric Passport Launched

As a front-line border country of the EU, Bulgaria has to deal with non-EU nationals wishing to enter the EU, at its border controls. This makes the introduction of the more secure biometric forms of identification a priority. Bulgaria originally agreed to include biometric data in all its identity documents, including passports, ID cards, drivers' licenses as well as residence permits for foreigners, by January 2007, as a requirement for joining the EU. Then the date was re-scheduled for mid-2009, but owing to further delays, Parliament had to extend the validity of 300,000 passports that were due to expire before or by the next planned launch date. The system was finally launched on March 29th 2010, but due to glitches coming from both the administration as well as the suppliers of software and materials, it was still not running smoothly, and has continued to have "teething" problems throughout the year. In spite of this difficult beginning, a million passports have been issued ahead of schedule, in only four months. A report in from the news agency, Novinite.com claims that 7,800 more are being issued every day.

Turkey's New Biometric Passport

Turkey's 1999 agreement to convert to biometric e-passports has finally been implemented. After some false starts, on June 1st 2010 Turkey launched the new ICAO compliant e-passports, which will considerably ease the passage of Turkish citizens through customs checkpoints and borders while travelling, and will also work towards Turkey's harmonisation with the EU.

Gemalto was asked to provide a personalisation solution and to train the staff who operate the system. They operate from two locations using their Coesys Issuance solution: on the premises of the Ministry of Foreign Affairs, and at the police centre in Ankara.

The identity page of the passport has all the visible details of the old passports as well as the bearer's photograph, fingerprints, signature and biometric features, which are encoded into the embedded microchip. At the bottom of the page, there is a mechanically readable, two-line space. These features provide a higher level of security and easier verification of identity.

Now everyone who is travelling, including underage children who were previously allowed to travel on their parents' passports, is obliged to have their own passport, and although the price was recently halved, it still costs 360 Turkish Lira (about €185) for a ten-year passport, making the right to visit another country relatively expensive in Turkey.

Azerbaijan's e Passport to be Provided by Trüb AG

The Republic of Azerbaijan has contracted Switzerland based company, Trüb AG, a leading manufacturer of ID cards, to supply their new, ICAO-compliant, biometric ePassports. The passports will have a polycarbonate data page containing an integrated contactless chip. The page, developed by Trüb, will be optically personalised using laser engraving and will include a number of integrated security features. A PKI system will be used to create the nationwide certificates which protect the sensitive information, i.e. the passport bearer's personal data, facial image and two fingerprints.

They are also supplying their Trackstar personalisation software and the laser personalisation machines that are needed for the job, along with providing maintenance and support for their solutions.

Trüb, with decades of experience in ID solutions, is also going to provide a consulting and project management service for the design and implementation of the complete system. There will be about a dozen personalisation centres nationwide, from where local authorities will issue the passports. The robust booklet is designed to last for 10 years.

A Biometric Passport for The Kingdom of Morocco

Gemalto has provided an end-to-end solution for the Moroccan Mint: Dar As-Sikkah (Bank Al Maghrib) for Morocco's biometric e-passport program, as part of a three year supply contract.

The solution includes the secure operating system, Sealys eTravel, and the electronic covers with integrated contactless microprocessors which contain the bearers photo and fingerprint. It also provides its Coesys Issuance personalisation solution as well as the installation, training and maintenance services. In cooperation with Moroccan company Netopia, Gemalto goes on to provide the Ministry of Interior with the Coesys Enrolment solution for citizen data acquisition and has implemented a skill transfer process for Netopia to accompany the start-up of the project.

Morocco, which began deployment of the new passports in December 2009, is the first non EU member to adopt the next generation biometric e-passports which include Extended Access Control, in conformity with specifications laid down by the EU, as well as being the first country in the Maghreb region to issue them.

India UID system

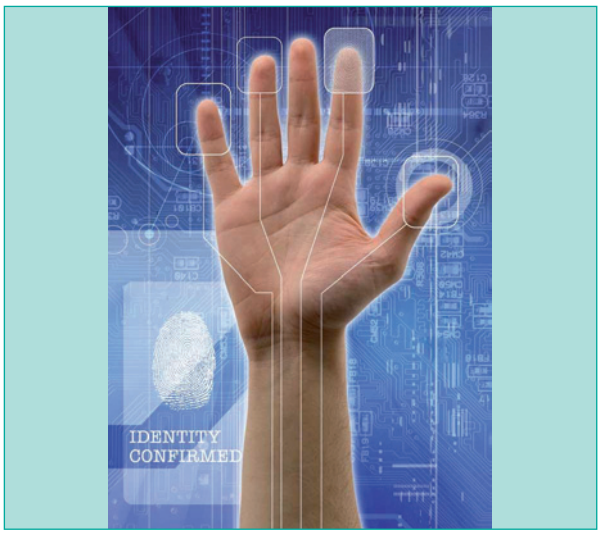
In an enormous project, at an estimated cost of between $2.2 and $4.4 billion, the Indian government has launched a plan to give each one of its 1.2 billion citizens, a card with a unique identification number; a UID card. It will eventually replace the many special-purpose identification cards that are currently required, such as passports, drivers licences, voting cards, healthcare or ration cards.

The card will contain several types of biometric data including multiple facial images, iris scans of both eyes and all ten fingerprints. The UID system will process hundreds of thousands of identity validation requests per second from the world's largest database. The system is so complex that it required a consortium of companies (Accenture, Mind Tree, Neurotechnology and Daon) to design the biometric data capture, categorization, storage and retrieval processes.

There are a number of advantages to the UID system, beyond eliminating the need to possess a wallet full of cards. One significant advantage is that it should put an end to the dilemma of many of India's poor, who are often unable to access needed services because they cannot prove who they are. Having a central database also simplifies the problems of migrant workers when moving between states, and means that drivers won't have to seek separate licenses when they drive around the country.

On the financial side there will be a reduction in administrative costs, and by the 'de-duplication' of databases and the cross referencing of current systems there should be a significant reduction in loss through fraud.

Critics of the system say that with a 30% illiteracy rate in India, some people won't be able to read the prompts while using the card. Others fear that the information in the database could be used to discriminate against people by caste, religion or birthplace, or they worry about the consequences should there be breaches in security.



RealScan live scanners and RealPass ePassport readers for South Korean project

In South Korea, The Ministry of Justice has implemented a fingerprint scanning system for foreigners. The South Korean Ministry of Justice has contracted Suprema Inc. to supply electronic passport readers and biometric live scan devices for their three-stage, nationwide program which aims to prevent the illegal entry of foreign nationals with forged identification.

The program, which began at Incheon International Airport, involves fingerprinting any foreigner who wants to enter South Korea. Suprema Inc., a leader in biometrics and ID solutions, are using their RealScan live scanners and RealPass ePassport readers for the project, the first stage of which was implemented in September 2010 in order to be in time to enhance security measures for the G20 Seoul Summit in November 2010.

The Ministry, which has already set up fingerprint and face recognition systems in Korea's 22 major ports and airports, intend to complete phases two and three by 2011.

Brazil's CAIXA to Use Biometric Identification System

Caixa Economica Federal (CAIXA) of Brazil have chosen Suprema Incorporated's RealScan-D fingerprint live scan system, for its biometrically enabled customer identification system, the initial phase of which covers its 300 major branches and posts.

One of the largest government owned financial institutions in Latin America, Ciaxa has plans to expand its biometric identification system to its 20,000 nationwide operations, including ATMs. They are implementing this system because they want to improve on security levels in financial transactions and branch operations.

The scanner, which has been used in large scale international projects (e.g. military project in Mexico, electronic voting system in the Philippines and public ID project in India) is a portable, USB powered device which has FBI IQS Appendix F certification.

New Zealand May Introduce Facial Scans For Visitors

Immigration New Zealand has started a trial of biometric facial recognition technology in order to verify the identity of visa applicants and travellers at the border.

Working with Australian biometric technology firm Daon, the trial is intended to evaluate whether using the technology, which takes a photo of the person applying for the visa and then uses it to confirm the identity on their arrival at the border, will make passenger processing any faster.

It is a short term trial, separate from the Immigration Global Management System, which is not being deployed operationally. Head of Immigration, Nigel Bickle, said that any decision about whether or not to purchase biometric systems is at least 12 months away.

Two Interesting New ID Cards

Safran's Morpho has produced a new fingerprint-based biometric card that can function as a non-repudiable signature. It has the same legally binding status as a handwritten signature, which makes it the first "Secure Signature Creation Device" as required by the 1999/93/EC Directive of the European Parliament and Council on fingerprint biometrics for strong user authentication in legal digital signatures.

The National Institute of Standards and Technology (NIST), as part of its fingerprint interoperability campaign, MINEX II, recently ranked the pioneering, biometric fingerprint technology, called Match-on-Card (MoC), first in the US.

Those who regularly have to use electronic signatures, such as legal professionals and finance executives, have welcomed the solution as they can now cut the time used for authentication.

SmartMetric have come up with a fingerprint-activated card called the Biometric Data Card, which can provide a high level of security, as well as portability, for an individual's medical history and full medical records.

Unlike other portable solutions that are very limited in the amount of data they can hold, the card has a significantly large, secure storage capacity and can store Gigabytes of data such as full EKGs, complete MRI and CT digital images in addition to other similar data, which comprise an individual's complete medical records.

The card only allows access after the patient touches the card's surface sensor, which triggers it to scan and match the fingerprint to the fingerprint already stored inside. As soon as there is a successful internal verification of the fingerprint, it will allow the relevant person, such as a doctor, to access or view the data contained within.

Samsung's Sortie into Science Fiction

Samsung have come up with the prototype of a new ID card design that they showed at the Las Vegas Digital Experience event in January 2010, which includes a little extra technology. By including a small, wafer-thin, OLED screen, it takes a leap from the ordinary right into science fiction. It looks almost like any other plastic eID card, and on the left hand side there is all the expected data: photograph of bearer, name, nationality, birth-date and expiry date of card, but on the right hand side there is a square, blank OLED screen. However, when the card is brought into close proximity with an RFID reader (ISO 14443), the screen is activated, and it generates a disembodied, rotating, 360° image of the bearer's head, making it a lot more difficult to forge an identity.

A spokesperson for the product said that the card is finished and ready for market. He explained that it was inexpensive because of "the commoditization of small OLED panels which are widely used today in mobile devices such as cell phones"

Securing Medical Identity in the USA

The Obama administration has earmarked a budget in excess of $19 million for the changeover from paper to electronic medical records. Another $1.7 billion has been allocated for fraud detection in the 2011 U.S. Health and Human Services Department budget.

With medical identity theft being one of the fastest growing crimes in America, it has raised some concerns about how to ensure that the security and privacy of personal data is properly controlled. One incident of note, (but not the only one) which illustrates the need for a serious improvement in security, was the loss of a hard drive— by health insurance plan, Health Net— which resulted in the loss of seven years of personal and medical information about 1.5 million of their customers.

There are concerns about whether the right information is being linked to the correct patient, either through genuine human error or through deception. Often, patients are only required to give a verbal assertion of who they are and what cover they have. Linking to the wrong record can lead to incorrect diagnoses and medical complications, with an estimated 195,000 deaths occurring annually due to medical errors. Booz Allen Hamilton said in the report "The Medical Identity Final Report", "...technology solutions such as biometrics, smart cards or electronic patient records may be able to assist providers in verifying patients' identities based on past histories, demographics or facial photographs".

According to a paper written by Smart Card Alliance, "Medical Identity Theft in Healthcare", solutions for identity management incorporating smart card technology, could be put in place without having to "reinvent the wheel". They believe that using strong authentication and data encryption are the way forward.

Smart cards have a number of data encryption enabling capabilities, e.g. key generation, secure key storage, hashing and digital signing. They can also add strong authentication capabilities that ensure only authorised people can access it. Advantages that smart card solutions can bring include the fact that signatures originating from a smart card are more credible and have greater legal stature, so they could be used by doctors to sign orders or prescriptions; also their portability – they stay with the doctor, reducing the opportunity to use it fraudulently, if, for example, it had been on a computer. From a patient's point of view, holding a smart card would give them more control over when, where and who can access their PHI, as well as providing security during the transmission of that data to healthcare systems.

Biometric Security Makes People Feel Safe

Unisys Corporation recently conducted an online poll to find out which form of identity verification they trusted most. The actual question was, "Which do you believe is the safest method to prove your credit card is being used by you?"
More than 300 people responded to the poll, the results of which are as follows:

63% felt that fingerprints were the safest method,
20% preferred identification from a photograph,
13% thought PIN numbers were best, and
6% wanted handwritten signatures.
In this electronic age, on any given day, the average person has to confront or combat at least two important personal security issues, firstly that of making safe financial transactions and secondly, that of protecting themselves against identity fraud. The results of the online poll show an increasing level of comfortability and acceptance in the use of biometric technologies for personal security in daily life.

This poll corroborated the findings of an earlier poll, (the April 2010 Unisys Index), which found that:
93% of Americans were prepared to supply a biometric to increase physical safety at airports, 65% would cooperate with full electronic body scans at the airport, and 55% would be willing to allow identity checks using biometric data, such as iris scans or fingerprints.

ruhlamat – your reliable partner for high professional smart card processing solutions.

ID CARD · SIM CARD · BANK CARD SOLUTIONS

From milling and implanting and implanting of the chip module through to contact and / or contactless chip loading as well as colour personalisation ruhlamat is your professional engineering and machine building partner for your costumised machine solution.

Our HD DOD industrial colour printing assures personalisation in brightest perfection in combination with extremely low consumable requirements. An extraordinary laser quality results from our sophisticated ruhlamat-software.

Our consulting, maintenance and service enables us to guarantee full support at any time.

AMERICA · EUROPE · ASIA
www.ruhlamat.com

ruhlamat®
solutions for your needs.

MACK GROUP

Citizen or Subject: The Politics of Personal Identity

By Philip Virgo, Secretary General, The Information Society Alliance - EURIM

" The issues of personal identity are central to a global information society in which we are routinely expected to conduct transactions with those whom we have not met before, cannot remember or may never physically meet. "

The issues of personal identity are central to a global information society in which we are routinely expected to conduct transactions with those whom we have not met before, cannot remember or may never physically meet. The supporting technologies, from smart cards, encryption and biometrics to secure and efficient databases and networks, have been in regular use for decades. The reasons for the current controversy over ID systems have little or nothing to do with technology developments: save in the sense that they may be used as an excuse for promoting a solution which serves political objectives.

The technologies may, or may not, work but they have to be operated by analogue mammals (hairless apes, alias human beings) whose standards of behaviour have changed little since writing first evolved in the deltas of the Euphrates (Iraq) and Yangtse (China), over five millennia ago. The oldest known writing looks suspiciously like a tax tariff for dealings in a cattle and grain market. The holy books of the monotheistic religions (Judaism, Christianity and Islam) contain many references to censuses, taxes and the means of identifying those who are to be respected. The teachings of Buddha and Confucius build on the wisdom of even older civilisations that recognized nothing was inevitable save death and taxes. Even the most primitive tribes have the wisdom to distrust strangers who take their picture or ask their name.

Today the first priority of our rulers is still to record their subjects and tax anything (or anyone) that moves or dies in their realm. Meanwhile the only identity tokens which their subjects value and respect are those which give credit in the market place. Today, that market place is increasingly international and electronic, with ordinary citizens, not just merchants and their agents, agreeing to transact with strangers on the far side of the world.

In consequence we have increased tensions between rulers, seeking to create and control local or national identity tokens, and their subjects - who want a variety of tokens according to whether they wish to obtain products and services locally or internationally without paying cash. We also have a tension between those who want high reliability tokens (to prevent possible terrorists boarding an airliner) and those frightened of being mugged on the way to the library or post office and having their identity stolen. From Brixton (South London) to Bogota (Colombia) no ordinary citizen carries more cash or ID than they really need.

The disciplines for Identity Management, including protecting transactions from local warlords - alias national governments - go back millennia. The traditions of "correspondent

banking" and of the notaries and scriveners who "authenticate" most global trade, go back to ancient Sumeria: where the laws were god-given and applied to the ruler. The traditions of government identity control go back to ancient Egypt, where the Pharaoh was a god. One of the most bitter subsequent clashes between the two traditions is enshrined in the story behind the Da Vinci code: Philip IV's attempt to expropriate the global correspondent banking operations of the Knight's Templar. Instead of heaps of gold all his troops found was files of incomprehensible paper – so they set about torturing the "bank managers". Even the transition to the electronic identities began over 150 years ago, with cable authentication routines, not just decades ago with smart cards et al.

This mature market has been regularly plagued by new entrants who believe they have "the answers" without being aware of what has gone before, the scale and nature of what is currently operational (including who is already doing what for whom, at what price and to what standards of accountability, responsibility and liability). Neither are they aware of what others are planning for the future, or what citizens, businesses and other "customers" would like or are willing to pay for.

Today the average on-line user is expected to remember passwords for around 60 "identity management" systems. Most enter the same personal information and try to use the same passwords for most. Surveys indicate, fairly consistently, that approximately 30% of population is concerned over their privacy etc. Most would like a choice, but assume they will not get one and would rather not draw attention by making a fuss. Some data indicates that as many as 10% of them give random answers, or use fictional persona, when they see no reason for giving their details to who-ever is asking. Most of us also carry over dozen or more machine readable cards, with a variety of chips, barcodes and/or magnetic stripes.

Current initiatives

There are a large number of current initiatives to introduce comprehensive integrated, federated and/or inter-operable ID management systems, proposed by a variety of players, with a variety of motivations. Few involve genuine choice or consent on the part of the "data subject": alias customer, citizen, victim, patient. "client" or "miscreant". Few relate to the experiences of governments in trying to keep electronic track of their "subjects" (from taxation and law enforcement to education, heath and welfare) or the private sector experience with running digital systems for:

- security printing
- credit reference
- age cards and loyalty schemes
- credit/debit cards, payment clearing and correspondence banking
- notaries, scriveners and supporting services
- fixed and mobile telecoms operators and payment services
- insurance (including life and healthcare)
- freight forwarding (land, sea and air: local, national and global)
- direct marketing: in all its forms: now including over the Internet
- sports and social clubs

as well as for central and local government, charities, voluntary agencies, law enforcement and the military.

Most initiatives ignore research on who we trust:

- doctors and nurses but not health service administrators
- banks and credit reference agencies before local government
- central government little more than pariahs – barely above on-line retailers and ISPs

Central to the sustainability and acceptability of successful ID management systems appear to be five R's:

- Responsibility (including ownership, accountability and duties of agents for owners).
- Registration (including confirming a claimed identity and linking an individual to their biography with biometrics and electronic credentials).
- Repair (when the registration and or credentials have been compromised or mistakes identified).
- Revocation (either full because of serious compromise or partial, e.g. moved from "good citizen" to "suspected fraudster" or "convicted criminal").
- Redress (who should bear the cost of repair and of compensating the victims in the event of compromise - whether deliberate or accidental).

There is little indication of academic, professional, legal or political agreement on "answers" to the questions of trust, but there are indications that some players have found "answers" that their customers, including end-users, find credible and acceptable. The basic questions can be summarised as:

- How are the five Rs (above), and the processes (including/especially the people processes) that support them, addressed (or not) by operational or proposed routines?
- What should be the roles of professional bodies, trade associations, politicians, regulators etc. in identifying and encouraging good practice?
- What should be the means of assessing whether the supporting technologies on offer are fit for purpose and used correctly?
- How could/should inter-operability be handled between different types of schemes (legal basis, management structure, application, ownership

etc.), including internationally, across jurisdictions, not just between similar schemes using different technologies?

- How could/should issues of issues of responsibility, liability, accountability and interoperability be handled across civil-military, public-private and international boundaries as well as across departmental or application boundaries?

Meanwhile the gulf between the approaches to Identity Governance of the NATO countries (largely driven by US post 9/11 paranoia and the aspirations of its would-be technology suppliers), and those of the private sector (especially finance), appears to be growing.

The current US Federal Government initiative has its roots in the confusion of 9/11 itself - when shoot-outs between federal agencies which did not recognise each other's identities were only narrowly averted, and emergency response teams were denied access. The subsequent refusal of access to those carrying fuel for the standby generators nearly led to a total collapse of communications (mobile as well as fixed) in New York. The US drive to impose their new approach on their NATO partners and supply chains has reinforced the current UK Cabinet Office attempt to meld the many British government working parties on ID systems into one: at the same time as they have scrapped ID Cards and Contact Point, dropped DWP's CIS database as a fulcrum for rationalization and fired the lead contractor for e-Borders!

Every Directorate and Agency of the European Commission feels the need to have an initiative, whether on the grounds of privacy, data protection or security – with little or no obvious co-ordination, let alone public or business support – other than from those bidding for consultancy or research business. Meanwhile the residents' cards of most EU states provide more efficient and accountable public sector identity regimes than the UK or US appear to have considered. Perhaps that is because so many have experience of totalitarian regimes.

The limitation of current UK Cabinet Office ambitions to addressing systems to identify those who work for government (including defence contractors etc.) is a good idea, given the obvious cost savings and operational efficiencies that should arise from culling those that are known to be inaccurate, inefficient and insecure. The decision not to extend the approach to cover all those who under statutory powers (not just law enforcement) might claim access to your home, business or computer systems, is unfortunate but understandable. It is not easy to provide routines that would enable a pensioner to check that the caller really is from British Gas and not another would-be distraction burglar, or for an office receptionist to bar the way until the Head of Security has arrived to check that the plain-clothes team really is from Health and Safety, Law Enforcement or the Tax Authorities.

While requiring that identity credentials of government officials have common roots may make good sense to those with military backgrounds, it also leads to vulnerabilities which the financial services industries have learned to avoid from centuries of experience (fraud and malpractice by trusted insiders). All security breaches at the Olympic Games have been carried out by those with impeccable credentials. Would the routines currently being promoted really help prevent a slaughter of the innocents when the security forces of the world shoot it out in London in 2012 after some-one mistakes fireworks for a bomb attack?

The last time that London hosted such large numbers of foreign security staff was 1066 at the Coronation of William the Bastard. It descended into chaos when the Norman guards outside Westminster Abbey thought the "acclamation" was an attack and set fire to the buildings round the Abbey to smoke out the "terrorists".

Before the General Election, Eleanor Laing MP, then the UK opposition spokesperson on identity issues, presented a ten-point draft action plan. It went down well with civil liberties groups, but like a lead balloon with most government officials and their would-be suppliers. It began with the assumption that we are citizens, not subjects and should own and control our own credentials and be able to choose the intermediaries who we trust to manage them. That would fit with long-standing financial services models for inter-operability between schemes where the issuer of the "credentials" is accepting liability under contract and/or common law tort. It would fit with voluntary residents cards issued by councils to facilitate rapid, uncharged response to enquiries or access to services (libraries, leisure facilities, travel etc.). It would not fit easily with claims to statutory immunity in the event of abuse or compromise.

The all-party Information Society Alliance (www.eurim.org) agreed to address the issues raised by Eleanor as part of their work on Information Governance to help the next government. They also plan to look at these in an international, not just UK or European, context.

For further information please visit www.eurim.org

ID Credentials: Governance – the missing link?

By Andrew Henderson, Wychwood Consulting Ltd

The UK has recently seen both the "bonfire of the quangos" in which a large number of these organisations have been swept away and a Bill enter Parliament to scrap the National Identity Scheme. It would therefore seem to be an odd time to be writing in support of a new quango, or governmental function. However there exists a problem around Identity and its management that exists whether Bills are passed or not. The problem for identity in the UK remains and it is this: From a consumer's point of view I have too many online IDs. I have therefore defaulted (for example) to three possible identities on the basis that I will only have three attempts to get my log-in right. I hand the components of my identity (User Name and Password) to many websites with little or no redress if things go wrong. There is no independent governance or regulatory authority to protect me, the consumer.

Every web-site that stores any sort of data on or about us requires us, the users, to register with a user name and password. In the UK it is made slightly easier in that many sites just require the E-mail address as the User Name. This makes it straightforward for me to remember, and for the website to contact me. It also makes it easier for the hacker who can harvest e-mail addresses in so many different ways. One large UK Bank even encourages you to write down your User Name, which they have sent you in the post. On the one hand this means a User Name generated, presumably, randomly and in a secure environment. On the other hand bank mail can be easily intercepted, a canny postman just needs to recognise the return address on the back! Furthermore, by writing the User Name down and leaving it, as encouraged, somewhere near the PC, the poor old user has just introduced an obvious vulnerability.

The problem that of having to remember multiple user names and passwords, has been tackled then by end users in one of two ways:

- Write them down either in your diary or by the PC on a Post-it sticker
- Default to one or two standard ones that you can remember.

This has introduced two basic vulnerabilities, on top of using one's email address as the User Name:

- Written down passwords which can be copied or stolen easily;
- Re-use of one of two passwords constantly which are vulnerable to hackers.

To meet this demand a number of companies have sprung up offering password vaults or other mechanism such as Bugmenot or Passpack. Indeed a survey in 2007 in PC Magazine cited the following as the ten most used passwords:

1. password
2. 123456
3. qwerty
4. abc123
5. letmein
6. monkey
7. myspace1
8. password1
9. blink182
10. (your first name)

What is happening then is that the consumer is being forced into insecurity in order to meet the demands of the various web-site owners. As mentioned, some try to get round this by issuing you with your User Name, but passwords by definition must be unique to the user and generated by the user. The balance between security and convenience is tilted in favour of convenience.

Some few have gone to pattern recognition on the basis that human beings remember patterns and sequences before they learn to recognise alphanumeric characters. However the ubiquity of the PIN number in particular has made this route a hard sell with little take up so far.

The problem that is left is a simple one and gets us back to the beginning of this article, lack of governance. If we take it as read that the user must generate his own password, what happens if it goes wrong. This can be in one of two ways.

Firstly, if the user cannot remember the user name or password and is therefore denied access to his data, who is responsible? Most websites do run a simple restore system based on the assumption that the user is at their PC signed into their email provider. Of course, should this be a malicious Third Party then they are handed the crown jewels. For most of us, it is inconvenient when we forget a password and need to wait for it to be restored. It can become a nightmare though when dealing with a bank, which may require you to go through the registration programme all over again.

One could reasonably argue, prima facie, that the user generated the User Name and password and is therefore responsible. However the user has not been given a genuine choice in terms of which particular User Name he may wish to use or the make up of the password. For instance, many websites will only accept alphanumeric characters and not speech marks or other available ones. If the user were responsible for providing their User Name and password of choice then the situation would be different.

If, by denying the user access to data because they forgot the key sequence of User Name and password, that user suffers loss to whom do they go for redress? In the event that a Third Party impersonates them, how does the user restore their identity and the rightful link to it?

Secondly, if that password is captured by a Third Party who will set about redress or restitution of any damage? Many of us, when purchasing online, will have got to the point that we are asked to enter three numbers from a set range, of 6 or 8 static ones. How many times does a hacker need to watch a regular online purchaser to capture all those static numbers?

This is where governance becomes important. Whilst politically not someone who supports the clunking fist of the State, the lack of an independent regulator for the identity market is beginning to become glaring. We were promised an Identity Commissioner on the back of the UK National Identity Scheme and Sir Joseph Pilling started in this role in October 2009. The role is however clearly linked to the Scheme and as the Scheme is now dead as soon as the Identity Documents Bill is passed to repeal the current Act, then the role will cease. There is no suggestion that the role might actually be changed to act as an ombudsman or regulator in spite of a growing market in Identity Management.

The purpose of the regulator is generally to protect the consumer. This may be through pricing policies, competition policies or general regulation to ensure that a market operates fairly. In this particular case though, in the UK at least, the private sector not the State is being encouraged to provide identity services. What therefore happens if a crime is committed or even a simple mistake such as the corruption of my data?

As a consumer, to whom do I turn for redress? I would have to take it up with the commercial organisation concerned. This process is a cost to the provider and therefore likely to be low on the list of commercial priorities. However it is important to remember that governance does help to create confidence in a market. There are examples where this has been lacking and unscrupulous players have entered the market or even helped to create it. The resulting financial loss suffered by the consumer has led to retrospective governance. Whether these are scandals concerning pensions funds, time share or the mis-selling of endowment policies, the horse has been allowed to bolt first before the door has been shut. As regards Identity Management, there is now an opportunity to act first and put a system of governance in place to provide a level of regulation that will instil confidence.

I believe that there is a natural reticence amongst many British people to hand over their personal data which form the components of their identity to be managed by a 3rd Party. The only documents that we have traditionally had are our Passports and Drivers Licences. Before the introduction of the Biometric Passport, the holder of the passport managed his or her own identity records. Passports were issued on the basis that the document itself was both correct and legitimate. If you wanted a new one because the old one was lost or stolen, your identity was not compromised at the Passport Office end because they did not hold your data in the first place. They relied on the end user re-applying as if from scratch.

Many new markets have sprung up in the technology revolution that has taken place over the past few years. Most of them are online versions of more traditional offerings. They rely on the international nature of the internet and its timeliness to offer global services. This also means that many UK consumers are lodging their identities with organisations outside the UK. How do we therefore deal with international governance?

In an EU context, there is work in progress and cross-border identity is being approached from a collaborative viewpoint. Whilst there is a long way to go, it is not unfeasible that a UK online provider who does business in Belgium would use the Belgian National ID card as the identifier. This changes the relationship between the consumer and the online provider. In this case the consumer presents their credentials and these are accepted by the provider. This gives the consumer the power to choose their identity and re-use one in which they trust. There is clearly a benefit to international engagement on this topic.

If we take a step now and imagine a UK in which we as consumers have access to an identity credential that we can create ourselves and use, then the boot is clearly on the other foot as regards the problem of a plethora of user names and passwords. The governance might in itself be easier in this other world. This is partly because it would help to encourage and create a market for organisations to issue out credentials and manage identities on a commercial basis. Thus we might as consumers chose two (one main one and a backup) as this is easier than the situation that we currently have.

Secondly, one can imagine a number but not a large number of organisations offering this type of service. There is, commercially speaking, an attractiveness in the critical mass of large numbers of consumers using X's service over Y's. It is also likely that, as happens in so many marketplaces, only a number will survive. Again the critical mass will drive commercial organisations to merge or acquire in order partly to spread costs over a larger user base but also to make it easier for the online providers of services to hook up to them. If company X has 2 million users and Y has only 10,000 then X is likely to attract more online service providers. Indeed some markets may combine such as banking to offer a single service based on a common platform. There are plenty of models for this such as SWIFT or LINK.

In sum then, the current situation cannot simply go on and on. The consumer is fed up and it will only become more difficult. Governance at the right level can help to create the confidence necessary to build up a market that allows consumers to choose whom they will engage with to pre and manage their identity and credential. Will the UK Government step up to the mark?

For further information please visit www.wychwood consultingltd.co.uk.

Digital Identity - A Radical New Approach

By David Watson, Business Compliance & Recovery Management Ltd.

"One of the main problems in using multiple sources of identity information in the 'real world' is that there can be variations in recorded information .."

Introduction

There can be few people in the developed world that are not familiar with terms such as 'online fraud' or 'identity theft' whether or not they regard themselves as being technology literate.

Any serious newspaper carries daily stories of the latest data breach by government, large corporations and most worryingly the military. The problems are many and varied, and the journey taken to reach such a woeful state is complex but the current approach of layer upon layer of digital 'sticking plasters' simply hasn't worked, and a fundamental re-think is required.

Two of the major problems in the digital world are:

- data breaches, meaning that individuals are becoming increasingly alarmed at the erosion of their privacy as their identity credentials and personal data are subject to unauthorised access or use:
- Proving your claimed identity to someone else's satisfaction.

In the former, partial or complete databases of personal information are lost or become accessible to unauthorised people. Because these databases contain personal data, they can be used for identity theft or other crimes.

In the latter, if any party in a digital 'exchange' does not know you, it is difficult to prove to those parties that you actually are who you claim to be to their satisfaction. This is also increasingly the case in the 'real' world for such tasks as opening a bank account, claiming a benefit, and a host of other tasks.

Solving both of these problems can provide a level of trust needed in a digital exchange and protect identity and attribute information about an individual.

A Brief Overview of Proving Identity

Simply put, an identity is a set of characteristics or attributes that allow one person to be identified from another.

We are whom we ***claim*** to be.

Before the days of the Internet and when interactions[1] happened within a village, everyone knew each other and so any interactions between members of the village were

between 'known' individuals. Anyone who had a problem with any interaction with another villager would resolve the issue locally as everyone knew each other.

The most difficult time was always a person's first relationship being established as it introduced an 'unknown person' into the known environment who had no existing 'trust'.

When interactions took place between individuals from different villages, a level of trust and accountability had to be established.

Taking this analogy further, we were able to trade overseas as a Lawyer in one country was contacted by one interacting party who then contacted a Lawyer he trusted in a different country to represent his client (the other interacting party). In this way, a trust relationship was built between the Lawyers and their respective clients, and the Lawyers themselves, creating a 'chain of trust'.

This system of using 'agents' in differing countries is still used in traditional trading. The most striking examples being the Chinese 'Chop' system, the 'Hawala' system in Pakistan and Afghanistan and the 'Hundi' system in parts of the Middle East. Money is transferred between trusted agents around the world, totally bypassing the traditional banking system – and thus any traceability. Any disputes in this system, which has been working effectively and efficiently for hundreds of years, are promptly dealt with.

The UK Home Office (in 'UK Identity Fraud, A case Study', 2002) identified three basic identity components:

- Attributed identity;
- Biometric identity;
- Biographical identity.

This can be likened to the traditional 'something you possess' (biometrics and attributes) and 'something you know' (biography).

Today, there is the need to prove frequently that you are who you claim to be in an increasing number of situations.

Fifty years ago, to open a bank account, it was common that someone you knew introduced you to a Bank Manager that they knew as a prospective customer and started a chain of trust that was independently verifiable. I well remember my father taking me to the branch he had banked in for twenty years, introducing me to the Bank Manager (who was one of his patients), and arranging for me to open an account before going to University. I had to show my University acceptance letter, details of my digs and my father guaranteed my overdraft. The bank really did 'know' their customer.

Today, the same process does not exist. To open a bank account it is still necessary to prove one's identity to help prevent money laundering and identity theft[2].

Using the Financial Markets as an example, the 'Know Your Customer' (KYC) process is the due diligence and bank regulation that financial institutions and other regulated companies must perform to identify their clients and ascertain relevant information pertinent to doing financial business with them. Whilst this is laudable, they do not actually 'know' their customer in most cases, there merely check a range of offered documents and perform some online checking. The Bank Manager with local knowledge has been replaced with impersonal credit scoring and arbitrary documentation to support a claimed identity. The process has been 'dumbed down' to something an outsourced vendor can do and that the responsible party can show to assure the Regulator has been adequately performed. Metrics do not demonstrate effectiveness!

The range of documentation to support claimed identity accepted varies from organisation to organization requiring you to identify yourself. Many of the documents used are not primarily identification documents but are used as such, a driving license is a permit to drive, not necessarily a proof of identity, and likewise a passport is a travel document.

One of the main problems in using multiple sources of identity information in the 'real world' is that there can be variations in recorded information (either accidental or deliberate) that make computerised matching of identity credentials problematic. The general rule is that all documents have to be:

- Accurate;
- Current (recent for bills or still current when issued for a specific duration);
- Matching (i.e. containing identical information)[3].

Manual matching, whilst possibly able to interpret these variations, is well nigh impossible given the range of information to be checked and the amount of identities to be processed.

The types of documents used to support a claimed identity vary, in order of strength of claimed identity, from:

- Government issued primary documents (typically a registration of birth or citizenship);
- Government issued secondary documents (typically containing a name and photo);
- Commercial documents showing name and address (typically a bank statement or utility bill);
- Letters from government departments or 'reputable persons' (typically a social worker, Police Officer, Minister of Religion.

At the bottom of the pile are club membership or loyalty cards. Each document performing the required role, even if it was not necessarily the original intended role.

A Brief Overview of Digital Identities

The first digital identities evolved approximately fifty years ago with the first computer. Prior to that, we all had real identities and the process of establishing and verifying an identity had evolved over centuries.

In the early days of computing, there were few users of mainframes; these were all in secure storage with access control. Generally, all of the users knew each other, so the chain of trust was present. They performed very few specific tasks and were typically run in batch mode with little user interaction. They were known for being expensive and so utilisation was closely managed and they were seen as slow to adapt to changing business needs and inflexible.

User Identities and passwords were used mainly for billing purposes. Any outsider trying to access a mainframe was immediately identifiable.

To overcome the inflexibility issue, and to allow business departments to have control over their own processing, whilst at the same time reduce costs, the mini computer was developed. This removed the ability of the 'Data Processing Department' to hold the company to ransom, however the confusion of central control and slow rate of change were linked and the idea of decentralisation being the key was pushed by vendors and the customers bought it. This meant that they had a cheaper computer to acquire, had networking and the illusion of business driven deliverability. What was ignored was the fact that centralised control and security were being eroded.

User identities and passwords, originally primarily used for billing, were now used for identification and authentication over a networked domain that had less security and control, and were then being assigned to unknown individuals. The chain of trust was starting to be eroded.

Business still thought the mini computer was too slow to respond to changing business needs and was too expensive and so the PC was developed and the desktop empowered. Suddenly almost all central control was gone as users could (and in some cases, did) run an organisation from their PC bypassing centralised systems.

This circumvented much, if not most, of the centralised control and security that previously existed. Instead of addressing the issue of speedier response to changing business needs and reducing the cost of development, a cheaper empowered desktop was implemented with local processing.

User identities and passwords still had changed little, even though their requirements had changed massively. No-one took a step back to see that the current identification and authentication process was appropriate, especially now networking between organisations was prevalent and growing. The problem had subtly transformed from controlling a login to legal proof of identity – we did not recognise that to our cost.

The theme of 'we now have the right solution in a new approach', rather than fixing the problems, was recurring. Suddenly everyone was jumping on the IT bandwagon, the whole notion of who was doing what with whom, where, under what jurisdiction and how remediation was addressed in case of problems was forgotten in the haste to 'get on board the e-train'.

In the 1990s, the internet arrived properly. Suddenly a system that was designed to be 'closed' and for the military and academics was thrown open to the world at large. Central control was almost non-existent and global interaction was facilitated, and we were only bothered about logical access.

User identities and passwords were still in use and few people could ever determine whom they were ever interacting with over the internet. It was best summed up with the famous cartoon 'On the Internet, Nobody Knows You're a Dog' by Peter Steiner.[4] Whilst the internet had enormous benefits, it had opened the world to identity thieves, hackers, paedophiles, malware writers, 419 crooks and a host of other criminals who were able to exploit it, extending their reach, whilst remaining anonymous. We had created a criminal environment unrivalled in history as anyone could be anyone they wanted to be on the internet with little fear of being detected, have their real identity discovered or even be prosecuted.

Centralised Databases

In the post 9/11 world specifically, and in many cases before it, a number of organisations held centralised databases of identity credentials and other attributes.

Multiple government agencies held individual databases for their own purposes – often unsynchronised with multiple duplicated data held in them.

The same was true for a number of commercial organisations.

There are a number of centralised databases that are now proposed (or already exist) that are to become national registration databases.

With all of this information in one place, they are a tempting target for anyone with criminal intent.

In 2007, the UK Chancellor Alistair Darling apologised for what he described as an "extremely serious failure on the part of HMRC to protect sensitive personal data entrusted to it in breach of its own guidelines". MPs gasped as Mr Darling told them: "The missing information contains details of all Child Benefit recipients: records for 25 million individuals and 7.25 million families."[5]

As can be seen from the above, it is quite a simple matter to lose details of 25 million individuals on two CDs.

This is merely the tip of the iceberg, and individuals are becoming increasingly concerned about failures to protect data, specifically their personal data.

It is interesting to note that some jurisdictions forbid centralisation of records for historical or other reasons.

It is also of note that the databases are usually only valid within a specific jurisdiction and there is no consistent interoperability between countries and jurisdictions.

Where these types of databases are used, there is always the assumption that that data held on them is accurate, when numerous studies show that this is not the case. This inaccuracy can prejudice the subject and in many cases is well nigh impossible to correct once recorded in the database.

It is too often the case (as Carol Beer in Little Britain would say) that the 'Computer says "no"' and that is the end of the discussion as the computer cannot be wrong!

In the extreme, if records are lost or seriously wrong on a national identity register, it is possible to lose your identity, and become an 'un-person'

" The range of documentation to support claimed identity accepted varies from organisation to organization requiring you to identify yourself. "

Identity Theft

Identity theft is one of the fastest growing crimes on the planet. The most recent figure was published on 9 October 2008 for the UK was estimated the annual cost of identity fraud to the economy at £1.2 billion[6].

According to an article in Forbes Magazine, identity theft and related fraud were up considerably in 2009 with 11.2 million victims for an estimated cost of $54 billion U.S. dollars.[7]

Figures of a relative magnitude will exist for other countries around the world, but they are all claims – no one really knows the true cost as crime figures are never fully reported and are always aggregated or processed to fit the reporting requirements of the organisation or author producing the report.

It is probably appropriate to say that the losses are truly enormous, growing and no one really knows the full scale of the losses – no matter what is claimed.

Today

So after fifty years or so of computing, where are we today in terms of identity, verification of identity, trust and meeting business requirements whilst protecting individual privacy?

We are at a position where:

- Identification and authentication (verification) processes are not always appropriate for our needs. We need to be clear when logical access is adequate and where legal proof of identity is necessary.
- Individual control over personal data has almost totally been lost;
- Personal control over identity has been almost completely eroded;
- The available tools mirror the limitations of the technology at the point of design;
- The IT Departments, IT Vendors and digital world generally forces their solutions and behaviour on us, rather than enhancing and enabling our human interactions;
- Typically, IT departments design systems and the business has little knowledge of their real requirements. It is often unable to articulate them or is bulldozed into vendor-supplied solutions. This leads to massively flawed solutions that often tend to pay scant regard to legislative and regulatory requirements or business best practice in the name of progress;
- Unauthorised disclosure of personal data is an every day event;
- We are often unable to verify a new individual's identity if we want to undertake any digital exchanges with them
- We see spectacular project failures both in government and commercially;
- The list goes on…

We still have not learned that IT Functionality is there to serve the business – not dictate how a business should be run.

A Radical Solution – What we Need

To start to rebuild trust in the digital world needs a radical solution – not more 'digital sticking plasters'.

To paraphrase Einstein:

'The thinking that got us into this mess – is not going to be the thinking that gets us out of it'

We need a solution that, in no particular order:

- Addresses business risks that should be managed and resolved by the business and not an IT Department or IT solution vendor;

YOUR PARTNER FOR SECURE ID CREDENTIALS AND SOLUTIONS

Secured Artwork
Innovative credential design
Advanced security features
Secure personalisation
NagraID Bio-platform
Consulting

NagraID offers tailor-made solutions based in multi-application smart card solutions including high security printing features with contact and/or secure contactless technology, and has developed a unique and patented process to manufacture ISO Display Cards for citizens ID's and secure ID's use applications.

We support also Citizens ID programs with our NagraID Bio-platform that is an ideal solution for rapidly and safely deploying applications such as national e-ID's, e-Health and other ID programs. The core software of our Bio-platform solution are based in the latest technologies available on the market (COTS - Commercial-Off-The-Shelf) and has been designed and integrated transparently with other information and business systems.
This approach insures that the system provided has robust and scalable foundations that comply with current national and international standards.

National ID's
Healthcare ID's
Driver's Licenses
Resident ID's
Voter Cards
Employee ID's ...

Display cards
... for the new generation of security ID's

Your contact for Government solutions:
Government@nagraid.com

Secure Manufacturing Plant for ID Credentials

Nagra ID
a Kudelski group company
Crêt-du-Locle 10
2301 La Chaux-de-Fonds
Switzerland
Tel: +41 (32) 924 04 04
www.nagraid.com

SWISS COMPETENCE IN IDENTIFICATION

- Addresses individual concerns about privacy – not one that forces us to accept what the technologists decide is good for us;
- Allows an appropriate dispute resolution process and appropriate redress to be implemented in case of need;
- Allows an individual to verify another identity to their satisfaction;
- Allows individuals (or legal entities for whom the individuals work) to set the level of protection that they want for each and every digital exchange;
- Allows individuals to browse the Internet anonymously if they want wish – just like window shopping or browsing in a department store;
- Allows individuals to control their own identity and supporting attributes;
- Allows individuals to verify themselves to other interacting parties satisfaction, and thereby actually be able to assert that the 'customer is known' by judicious choice of verification;
- Allows parties to a digital exchange to agree and enforce appropriate contractual terms for every digital exchange;
- Allows users tools to allow them to manage their identity, from profiles, through attributes and security setting to any other personal settings that they wish to record or use;
- Can answer questions such as is this person eligible for a service without disclosing identity (a simple 'pass / go gate')
- Can provide on line or off line verification, as appropriate or required;
- Can start to rebuild trust in the digital world between parties that want to undertake digital exchanges of any type.
- Ensures that identity and authentication is at least a two way process;
- Ensures that technology that supports the required processes, enabling and enhancing them – not mandating how they should be performed;
- Ensures that trusted third parties should be of the individual's choosing, unless they are being used by an individual acting is a delegated role for a legal entity, in which case the legal entity should be able to choose them.
- Facilitates clear business rules being converted into technological solutions;
- Facilitates trusted third parties to either hold personal data (releasing it according to the specific terms agreed with its owner) or holding transaction data (an audit trail of known and provable integrity) that can be produced if needed;
- Increases security of personal data;
- Means that an individual does not have to disclose their identity until they want to and only enough attributes to satisfy real business need – rather than some arbitrary nice to have concept of obtaining 'the more the better'
- Provides interoperability between countries where identity needs to be verified;
- Provides irrevocable proof of all digital exchanges undertaken by an individual as required to provide total traceability and accountability for actions taken with a given identity;
- Provides legislative and regulatory compliance within the relevant jurisdictions;
- Puts a business back in control of its business processes without abrogating responsibility to the IT Department or other technologists;
- Puts an individual back in control of their own identity;
- Reduces compliance risk;
- Reduces crime and specifically identity theft;
- Reduces data duplication and incorrect personal data being held for decision making purposes;
- Separates the identity of the person from their attributes – so that if a database is compromised – the identity is not:
- Where individuals can store their personal data in 'digital wallets' or 'personal information stores' under their control – and replace the technology used to hold them without loss of data or services.

Unless we can restore trust between the parties in a digital exchange, identity and identity verification will remain a technology issue and that just does not work in the real or the digital world.

So, in summary, can technology solve these issues?

Not in its current form – a radical rethink is needed but technology used appropriately can provide some of the building blocks to provide it.

[1] In this case, an interaction is typically an exchange of 'something' between two or more parties. This could be trading goods, exchanging information etc.
[2] Many 'Identity Proof' type documents state this, but as identity theft is one of the fastest growing crimes it might be reasonably assumed that this procedure does not work
[3] 'ID Guide, How to Prove Your Identity', Toynbee Hall and Barclays Bank.
[4] New Yorker Magazine, page 61, July 5, 1993 issue of The New Yorker
[5] http://news.bbc.co.uk/2/hi/7103566.stm
[6] http://www.identitytheft.org.uk/cost-of-identity-fraud.asp
[7] http://www.crunchgear.com/2010/02/10/identity-theft-costs-rise-overall-while-costs-per-victim decline/

For further information please visit www.bcrm.co.uk

DOCUMENT AUTHENTICATION –

EMERGING COMMERCIAL APPLICATIONS

By Jeff Setrin, VP Engineering, Documetrics and Dr Mohamed Lazzouni, Senior Vice President, Engineering and CTO, L-1 Identity Solutions

The number of U.S. identity fraud victims increased 22 percent in 2008 to 9.9 million adults.
Source: Javelin Strategy & Research, February 2009 study

Merchants are paying US$100 billion in fraud losses due to unauthorized transactions and fees/interest associated with chargebacks, nearly ten times the US$11 billion cost incurred by banks and more than 20 times the total value of consumer losses.

Source: The 2009 LexisNexis True Cost of Fraud Study

Establishing that someone really is who they say are when they seek entitlements and services requires the analysis of multiple modalities of identity claims, including but not necessarily limited to:

- Demographic
- Biographical
- Biometric
- Document

In this paper we will focus on the 'Document' modality. Vetting the authenticity of a document represents a crucial step in establishing the veracity of an identity claim. The process of document authentication involves applying various means, manual and automatic, electronic and optical, to verify that presented identification documents (passport, driver's license, national ID, etc.) are legitimate. Machine-based automated authentication has seen significant progress in recent years.

Automated document authentication technology has traditionally been deployed in government applications such as border control and in vetting breeder documents when applying for a new identification document, the primary motivation being heightened security. There is growing demand for document authentication in commercial applications. Commercial enterprises such as banks and major retailers face increasing competition and unprecedented pressure to provide immediate gratification, even when performing high price transactions. These trends make potential losses from fraud greater than ever before.

The challenge is to effectively address security and financial risks without compromising business operations and customer service. Identity documents with embedded electronic authentication capabilities facilitate the increased level of automation and accuracy demanded by commercial markets. However, these advanced capabilities also mean additional costs that need to be justified by a clear business case. One such justification is to provide support for a combination of government and commercial services. With somewhat conflicting requirements, it will clearly take time for electronic identification documents and other forms of electronic authentication to completely displace more traditional forms of identification. In the meantime, a variety of authentication technologies and techniques must be creatively applied in hybrid optical-electronic solutions.

REQUIREMENTS

While commercial enterprises are concerned about security and the financial impact of identity fraud, these concerns are quickly overshadowed by the threat of incremental costs and lost revenue due to process complexities and degraded customer service. Government sector document authentication and identity verification initiatives are often driven by legislated regulations, but this is rarely the case in the commercial space. There has to be a convincing business case for the enterprise to take on a comprehensive document authentication initiative, and it's imperative to minimize the costs associated with deployment and operation of such solutions. Shared service offerings that cover the entire document lifecycle (issuance, usage, modification, and retirement/revocation) represent one approach. This requires shared infrastructures or, at a minimum, inter operable identity documents. EU eID initiatives preserve member state independence in defining appropriate solutions for electronic identification and authentication while requiring levels of interoperability across the member states. In the US, small government and commercial entities are turning to third-party service providers to issue custom identification documents.

ID document usage models must satisfy the needs or requirements of multiple stakeholders, each with their own focus, priorities and perceptions (see Table 1).

Stakeholder	Focus / priorities
Customer	Price, quality, and accessibility
Operations Staff	Transaction time, ease of use, and customer service
IT	Network/storage demands, and system deployment and maintenance
Fraud Investigations	Data privacy and identity verification
Business Management	Sales, margins, employee performance and customer satisfaction

Table 1

Specific requirements and challenges of moving from government applications into the commercial sector include:

- Heightened priority on customer service. Commercial businesses do not have a captive audience as is often the case for the government sector. Customers have many options for where to do their business and make buy decisions based on:
  - Price
  - Speed of service (accessibility to online and in-store outlets, payment options and transaction time)
  - Quality of product/service (reliability, accuracy, breadth of service offerings, etc.)
- Employee turnover and the use of temporary staff is more prominent. Less skilled operators require simplified user interfaces, operational processes, and a high degree of automation.
- There is no secondary support infrastructure for handling process exceptions and no time or desire to have front line operators adjudicate authentic - ation exceptions. Clerks need a simple process for authenticating the document, a quick pass/ fail result, and clear guidelines for reacting to either event.
- Network and storage IT infrastructures may not be prepared to deal with large document and biometric image components. Resource demands must be minimized through optimization.

Relative priorities vary between government and commercial entities (see Figure 1). For example, the implications of a security breach are normally far greater for a government entity while ease of use and customer service is of the utmost importance to the commercial entity.

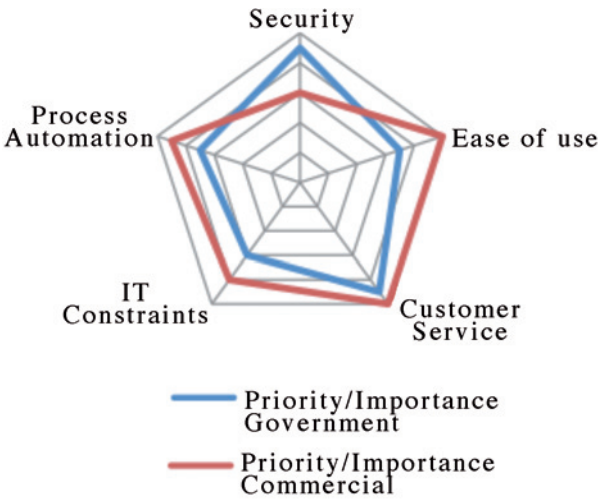


Figure 1

Unique benefits

Opportunities for the commercial enterprise to extend baseline identity verification benefits include:

- Customer Relationship Management (CRM) via collection of customer demographics including gender, age, nationality, and address. This information can be used to drive customer loyalty programs, targeted marketing campaigns, and product offerings at specific locations.
- The ID document can be used as the default membership card in tracking benefit entitlements and sales activity. The document can be registered into the commercial entity's database through an enrollment process where additional information such as the applicant's biometrics can be added to strengthen the security of the identity verification process.

Technology

The goals of automated document authentication are to move forensic document analysis from the back office to the front office, from batched or deferred mode to real-time, and away from manual or human processes.

The optimal technical solution varies depending on the nature of the documents, the available IT infrastructure, and the customer's business process. A multi-layered approach is called for to provide the flexibility required to satisfy diverse demands. First and foremost, authentication of the document

itself requires applying sophisticated electronic and optical forensic techniques. Optical analysis can verify the presence of expected security features and proper behavior when as the document is subjected to various non-destructive tests. Embedded data acquired from chips, digital watermarks, barcodes, magnetic/optical stripes and printed text is verified and crosschecked to verify integrity and consistency, and can then be directed to data entry applications. Security technologies such as digital watermarks are effective in detecting common ID tampering techniques such as photo substitution. The advantage of this localized approach is that there is no need for the network infrastructure or the time and cost associated with accessing external data sources and dealing with their imperfections (e.g. stale data and gaps in coverage).

Today's solutions need to fully leverage the enhanced capabilities of next-generation identity documents. With the shift from optical to electronic authentication, and increasing availability of the necessary infrastructures such as PKI, the industry is moving towards identification documents capable of supporting a blend of government and commercial applications. A multi-layered document security approach is necessary to ensure a flexible and robust usage model. Optical security features will continue to be prominently featured in new document designs, and will be quite useful in situations where a document's chip is not functional or chip reader equipment is unavailable.

Implementation challenges – managing exceptions

The ideal of a 100% accurate system where a Pass result conclusively confirms the document as authentic and a Fail result conclusively identifies it as fraudulent is very difficult to achieve. Document authentication systems, like other forms of analysis and recognition systems, are not perfect. At the highest level there are two types of errors.

Error	Impact
Type 1 Error / Passing a bad document	Potential for undetected fraudulent transactions with associated financial and/or security ramifications, but no direct impact to customer service and transaction flow.
Type 2 Error / Failing a good document	Potential for lost business, and degraded customer service due to extended transaction times. High error rates present risk of loss of confidence in the system.

Table 2

Undetected bad documents are highly undesirable, but it's important to remember that the primary goal is to catch as many bad documents as possible with minimal or no disruption to business operations. While certain stakeholders view document authentication as a solution to a critical problem, operations staff may simply view it as a new problem or burden that they don't have time to deal with. These people didn't need to worry about dealing with fraudulent transactions because most of them went undetected until after the fact or not at all.

Handling authentication exceptions is best left to skilled people who are largely dedicated to performing this function. Larger organizations may have trained people at each site, but in most cases this is a centralized internal function or provided through a third-party service. Service costs will vary depending on transaction volumes and response time requirements. Business rules can be established to institute local exception handling procedures such as repeating the document scan to ensure proper insertion, requesting alternate forms of identification, asking security questions, etc. The next option is to initiate a remote adjudication action, further extending the length of the transaction. While it may be acceptable for a bank to ask a new account applicant with a questionable document to return the next day to complete the transaction, a customer hoping to purchase a new cell phone might not accept this delay.

The process for responding to legitimate authentication alerts may also vary depending on business practices. A person presenting a fraudulent document is not necessarily trying to commit a fraudulent transaction. The fraudulent document may have been obtained to establish illegal residence and gain employment, and the bearer may otherwise be a law abiding citizen who poses no threat of illicit financial transactions.

> " A person presenting a fraudulent document is not necessarily trying to commit a fraudulent transaction. "

Most commercial operations lack a local secondary support infrastructure (see Figure 2) so there is an increased dependence on a centralized function, possibly an outsource service provider, for dealing with authentication exceptions.

As authentication accuracy improves, as it surely will with the emergence of electronic authentication techniques, adjudication time and cost will decrease.

Recommended best practices

Commercial markets demand a high degree of automation to achieve the simplicity and speed required to meet ease of use and customer service expectations. Recommended best practices include:

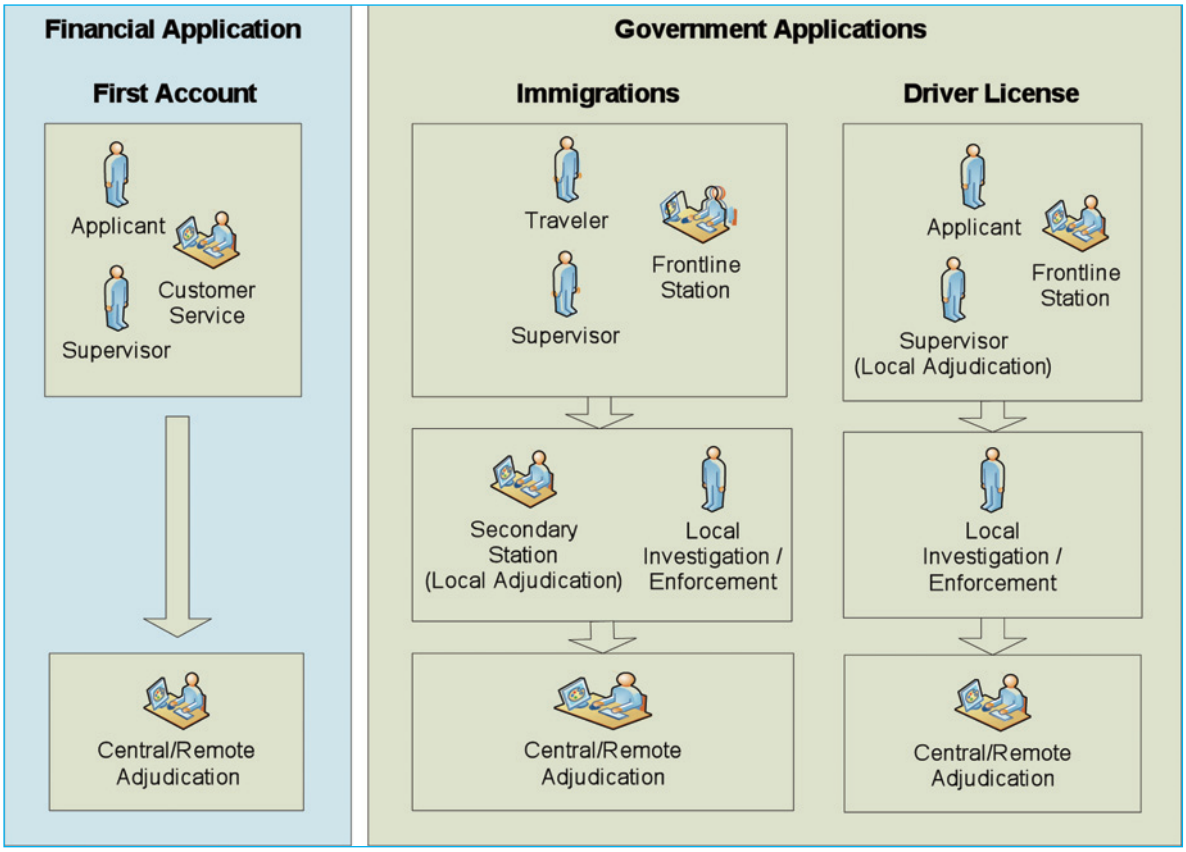


Figure 2

- Thorough business impact analysis that considers all stakeholder perspectives.
- Reduce operational overhead through selective application of document authentication based on business rules relating to transaction location (focus on high risk areas) and transaction type (new bank accounts or check transactions that exceed a certain value).
- Simple process for performing a document authentication transaction. Here ease of use focuses on the ergonomics of the solution. The physical actions associated with processing a document such as insertion and removal must be intuitive, flexible and forgiving.
- Simple pass/fail authentication result. Frontline operators should not be burdened with analyzing underlying causes of the result.
- Centralized function for processing authentication exceptions where response times can be tailored to business needs so frontline operations are not adversely affected.
- Optimized data acquisition and storage techniques that meet business requirements yet minimize IT network and storage resource utilization.

Economic considerations

In addition to a reduction in fraud related business losses, operational costs can be significantly reduced through automation. Forensics tests that would otherwise take a minute or more to perform can now be performed in a matter of a few seconds. Central support for exceptions adjudication can reduce overhead by as much as 90%. Data acquisition costs can also be reduced through automated machine readable data input.

Conclusions

We have learned the value of document authentication. While it is not a panacea it does address a critical need in combatting document and identity fraud, and can play a large role in national security and facilitating commerce.

Looking to the future, commercial applications may prove to be instrumental in providing the incentives required to achieve interoperable identity management solutions that facilitate access to both government and commercial services. The winners in a highly competitive landscape will be those that employ well-balanced document authentication solutions that address all forms of identity documents and the needs all of the host entity's stakeholders.

For more information please visit www.l1id.com.

eID IMPLEMENTATION: AN OPPORTUNITY TO IMPROVE THE RELIABILITY OF ALL FOUNDING DOCUMENTS

By Frédéric Trojani,
Senior Vice President, Government Programs,
Gemalto

When it comes to the question of implementing an eID program to improve the ability of each individual to exercise their rights and responsibilities, and even to ensure social justice, the fight against identity fraud clearly becomes a critical area in which progress must be made.

But what would be the point of issuing secure documents if the civil register and its source data are easy to falsify and even corrupt with an uncertain version history?

CHALLENGES

The development of electronic identification, (also known as eID), and its related eGovernment and eServices is based on building a secure infrastructure to coordinate efforts to improve the reliability of all documents issued. These documents enable individual citizens to exercise their rights and responsibilities via digital means. Clearly, document theft and fraud are sources of social injustice as the community may inadvertently allocate resources to an ill-intentioned individual feigning another person's identity, thus depriving the genuine citizen of that to which he or she is legally entitled.

The first element of reliability that one should be able to expect, to avoid creating a climate of mistrust across the eID program, is the theft-proof nature of the procedure involved in issuing and distributing documents.

Where do the weaknesses in the system lie? They are found at two stages of the document production process:

- Presentation of forged supporting documents when registering the application.
- Reception and validation of the application by the registrar, either when the application is registered or during the examination of the application before the document is physically produced.

Identity,
a powerful symbol of equality among citizens

Identity is the link connecting the individual to the community (Condorcet 1793).

Protecting identity against fraud or theft is the key to maintaining confidence in this link. It is crucial to be able to verify that a person is who he or she claims to be when exercising his or her rights and duties as a citizen. Digital technology has only heightened this essential need.

Identity, a powerful symbol of equality among citizens
In the 21st century, identity has come to express the differences between citizens. However, it was originally a concept that expressed their equality. When, in 1793, French mathematician and jurist the Marquis de Condorcet laid the foundations of 'social mathematics', he studied the relationship between the individual and the collective in an effort to formalize the foundations of the democratic system. In choosing the mathematical term 'Identity' to represent the algebraic concept of equality among citizens in terms of their legal rights and obligations, he expressed the definition of the word that has persisted ever since – the state of one thing being the same in nature as another, of two things being one.
In other words: One nation, constituted by the sovereign people and their chosen representatives. One republic. Multiple individuals who, by 'identically' accepting the rules of the community to which they choose freely to belong, attain the status of citizens.

Identity is a principle with two dimensions, and the link between the individual and the collective.

Benefits and operating procedures

This requires implementation of two sub-projects to contribute to securing these two delicate stages:

- Converting the civil register to a paperless system
- Producing secure public official cards

Converting the civil register to a paperless system

The central element providing proof of the authenticity of the identity of individuals requesting secure documents is of course the extract from the civil register.

Converting the civil register to a paperless system is therefore based on at least two main aims:

- The digital transmission of extracts via a secure channel, avoiding fraudulent actions by intermediaries with access to non-secure copies.
- Gradual creation of a digital repository of civil registry documents, which will rapidly become the parent database for all identification documents. Bearing in mind that it is always possible to adopt a proactive approach to speeding up the digitization of archives rather than simply waiting to receive document renewal requests.

For countries who consider their archive data to be insufficiently reliable, it is also possible to proceed with national registration in the form of a census campaign. Some countries have then opted for biometric registration, taking the view that citizens' digital and/or facial biometry remains the most reliable source for unmistakably identifying them. The 'one for one' biometric inspection is performed when a civil register supporting document is transmitted, thus enabling its authenticity to be verified.

A double opportunity: securing the source and setting up a pilot sample

When it comes to the distribution of secure documents, the advantage of starting by focusing on public official cards is also an essential point, ensuring the reliability of the requests received for secure documents, which will be electronically signed by certified officials, thus reducing the rare, but possible, temptation to commit internal fraud.

The second opportunity of starting with public official documents is that it also enables a pilot sample of the distribution of secure documents to be produced. This pilot sample has proved, in many countries who have started with this first step, a non-negligible advantage in that it enables reliability of the back office to be improved and its switch to digital exchanges to be speeded up. This offers an initial opportunity to improve efficiency and reduce processing times for government bodies. The on-line services that are then to be implemented will offer even greater performance.

Towards a biometric civil register?

One starting point when consolidating or harmonizing the civil register is to look for the unmistakable element with the greatest reliability which enables an individual to be identified. In many countries where names, addresses and dates of birth are standardized and reliable, this basis can be used as an identification reference system. Biometry is, in such situations, a simple attribute that makes it possible to secure the link between physical person and data.

In countries where semantic standardization work on citizens' names is not entirely finalized, we might reasonably assume that biometric recognition will most likely be the common element with the greatest reliability. This will as the basis of identification.

On this point, it should be noted that it is generally considered that although identification data is shared between the citizen concerned and the government bodies, the civil register data is however generally viewed as representing private data. Such data belongs to the citizen personally, who entrusts it to the state in the role of notary and archiver, and then presents it when requesting an official document issued by the state. The civil register, in this sense, may incorporate an individual's biometric data, as soon as this can be considered, barring accidents, as being permanently valid and reliable.

In the case of biometric databases compiled previously, the issuing of residence permits, new eID cards and biometric passports will be an opportunity to update biometric data and check the doubly unmistakable relationship of fingerprints to name held on civil register.

Securing the registration system

To prevent secure documents being traded as goods, officials working anywhere in the system will be provided with public official cards and, in their role as registrars, will personally validate each of the information exchange and modification stages involved in producing the document.

In conclusion, for the civil register sector: the first eID documents to be delivered, establishing an excellent pilot basis, will be public official cards. As the first documents to be registered in a secure manner, they will play an active role in supporting security throughout the document system.

The issue of consistency, reliability and harmonization of the civil register is a challenge at the very heart of citizen identification policy In Portugal. Here, the state has devoted several years to validating its civil register reference database. Portuguese citizens may have two surnames and two first names, for which they are able to choose, and change, the

We are Morpho now!

Morpho brings you the most innovative, complete solutions for high-end biometric Passports and ID Cards.

Morpho provides vast expertise and skills with strong local presence on all continents.
As market leader we already issued more than 30 million passports with a polycarbonate datapage and integrated chip and antenna.

The Netherlands, Switzerland, Ireland, Finland, Slovakia, Albania, and Croatia have already chosen for our Passport solution.

SAFRAN
Morpho

Formerly known as
Sagem Identification
Oudeweg 32
PO Box 5300, 2000 GH Haarlem
The Netherlands

Phone +31 23 79 95 111
Fax +31 23 79 95 180
www.morpho.com

order. Hamonization has been essential to obtain reliable, standardized, secure access to data and help combat fraud.

Anabela Pedroso, former president of AMA ("Agência para a Modernização Administrativa" – Agency for Administration Modernization), Portugal reports that when implementing eID it is essential to be aware of the naming standardization issue:

"The interoperability between services is not only technical, it is also organizational and semantic.
For example, when administrative services wish to interoperate, and prevent identity fraud which is ever increasing, the issue of the coding of names and addresses is tricky, and one which we recommend states about to issue their eID card address as soon as possible.
"We have had to finely review all our administrative registers to remove any redundancies from our systems and registers while keeping them independent from each other in order to respect privacy. It is a task not to be underestimated.

"For example, 'Who am I? My name is Anabela Damásio Caetano Pedroso. However I am on record as Anabela Caetano Pedroso, or Anabela Pedroso, or with my full name. If I am a foreign resident, from Europe in particular, I have the right for my name to be spelt correctly. There are over 390 different characters if we combine all the languages and special characters or alphabets from the 27 states.

"I may also have several addresses and some combinations of my name may be known at various addresses. For example, property purchased before or after marriage. Or even concerning healthcare and related rights.

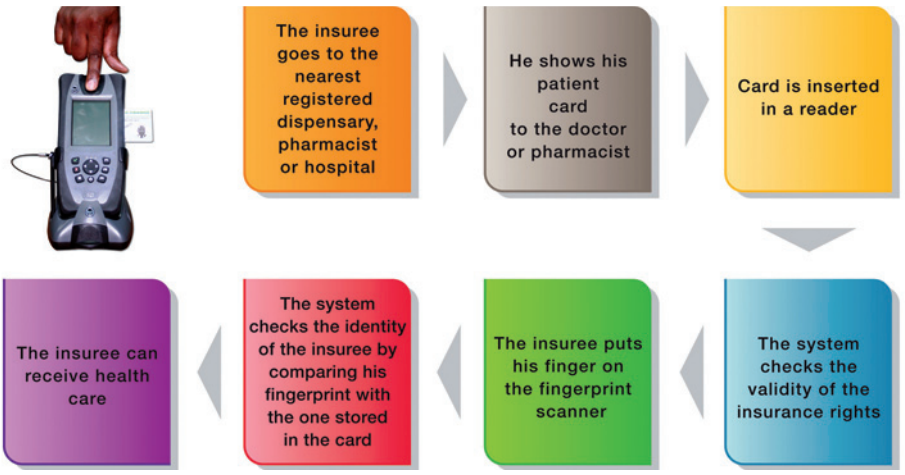
However it is citizens' right to keep these differences and administrative services must adapt while combating fraud. A compromise is necessary.

"We must simply remember that ID management is a lot more cultural than planned for the modern information process. These two social, and even economic, realities must coexist."

Identity is key in eHealthcare programs

Boualem Touati, IT director, Caisse Nationale des Assurances Sociales (CNAS) [National Social Security Fund]) Algeria, explains why identity is essential in eHealthcare programs: "The key to this is the need for robust identification so that we can answer the question 'who is paying for whom and for what?' It is essential for better rationalization of health expenditure, for checking purposes and, above all, for the sustainability of the social security system. It would be illusory to think that the supply of services could remain anonymous.
"Secondly, this identification highlights the importance of the original identity data including the central element providing proof of authenticity of the identity, which is the extract from the civil register.

"Finally, the unique identification efforts, such as those that we have made within the social security system in Algeria, must be able to be used in other national projects, by pooling identifiers and management of processes.
"We must obviously avoid the duplication of technologies, registering processes, verification, identity management, and so on, for major forthcoming national projects, such as the national eID program."



In Gabon, biometric match-on-card allows strong identification of the patient. No central database of fingerprints is needed as the control is done off-line. Even before the program started, it was clear to everyone that all resources should be implemented to avoid the health cover program turning into a centre of attention for the citizens of neighbouring countries and lead to its collapse through the fraudulent use of rights.
Beneficiaries must be individually identified so that access to care can be reserved for them. It has been decided that the identification of insured parties will be nominative with the implementation of a Gabonese individual health insurance number.

For further information please call: + 358 (0)9 8941 4602 or email: frederic.trojani@gemalto.com.

Biometrics – It's not what you know, it's who you are!

By Neil Fisher, VP, Global Security Solutions, Unisys

Managing identity is quickly becoming the dominant issue shaping the way governments operate, people communicate and businesses interact with their customers. But, says Neil Fisher, VP, Global Security Solutions, Unisys, traditional ways to prove your identity are becoming redundant.

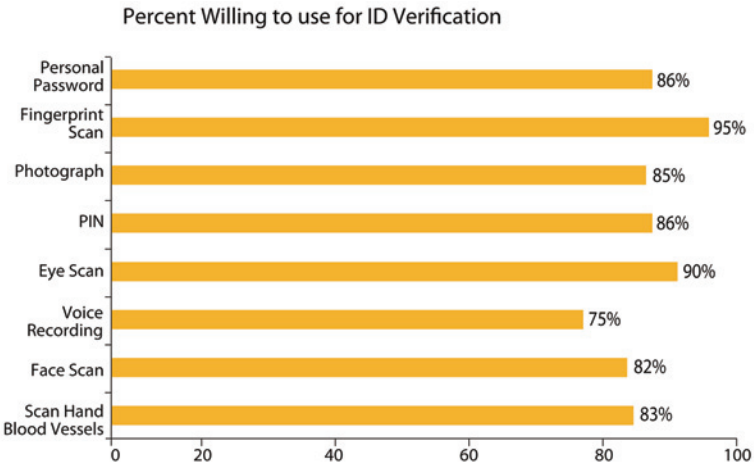
Protecting your personal information with 'what you know' is no longer good enough. In this digitised, Web 2.0 era it is now too easy to find out information like a birth date, address or mother's maiden name when they are freely posted on social networking sites like Facebook, LinkedIn and Twitter.

Additional measures of combining 'what you know' (eg PINs) with 'what you have' (eg smart cards or tokens) provide another layer of protection for consumers against identity fraud. But in some instances, where even greater assurances of identity are required, organisations are seeking even better protection via another layer, 'what you are', through the use of biometric technology such as fingerprinting, iris scanning and vascular technology. These identification technologies have the potential to improve both security and privacy - with corresponding benefits to consumers, corporations and government agencies alike. Consumers experience the advantages of greater convenience, ease-of-use and privacy in their interactions with trusted parties such as banks, airlines, and government agencies. Corporations and government departments thrive on stronger forms of authentication, improved security, less susceptibility to identity theft and fraud, reduced costs, and lower risk in terms of regulatory compliance.

It is therefore not surprising that we are increasingly seeing appropriate security measures being put in place to reduce exposure to today's complex range of security threats. According to the Unisys Security Index (www.unisyssecurityindex.com) – a global research report designed to help businesses and governments understand consumer attitudes towards financial, personal, internet and national security, 85 per cent of Brits are worried about identity theft (of which 55 per cent are seriously concerned). In fact we are more worried about ID theft than our ability to meet our financial commitments. These findings coincide with a report from the National Fraud Authority which found that each victim is stung for an average of £1,000 in credit or benefits and in most serious cases, it can take victims more than 200 hours – the equivalent of a year's annual leave – to resolve the problems caused by identity fraud.

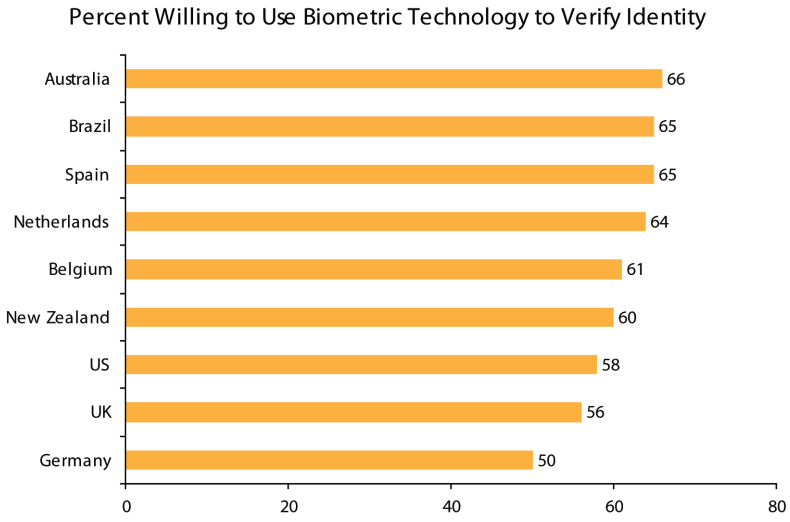
Given this level of trepidation, it's therefore not surprising that a previous wave of the Unisys Security Index carried out in April 2010 revealed strong public demand for innovative security techniques to prove our identity with better and stronger assurances. Public acceptance of biometric technology has rapidly been gathering pace; 91 per cent find the use of fingerprint scans to verify their identity with banks, government agencies or other organisations acceptable, up 16 per cent in the last year.

A recent Unisys online poll also revealed that consumers trust fingerprint biometrics over photo identification, PIN numbers or handwritten signatures to verify their identities when using a credit card or requesting personal information. Again, these results indicate increasing consumer acceptance of biometric technologies to secure financial transactions and combat identity fraud.



Combined, these findings provide compelling evidence that, contrary to mistrust of biometric technology, organisations which adopt these technologies and make their security measures transparent will take the lead in integrating biometrics in established security protocol. The success stories will be those organisations which invest in transparent processes and education to reassure the public that their data has been securely collected, respected and protected.

The public's willingness to embrace biometrics is driven by an inherent expectation that people should have the freedom to trade online and across borders whilst enjoying absolute security and protection. As the use of biometrics continues to mature along with public acceptance of the technology, innovation will inevitably expand into new domains and beyond familiar methods of voice, face, finger and iris recognition. One promising alternative is vascular recognition technology, of which Unisys is a strong proponent.



Vascular scanning technology is a rugged and robust tool. Infra-red cameras read the back of the hands from a small distance away. Verification is instantaneous and achieved when the blood flow pattern of the holder's hand matches the pattern of the scan stored on a smart card. The technology carries a high degree of accuracy, is easy to use and overcomes most physical disabilities. Unisys has already integrated vascular credentialing biometrics into its security credentials procedures to identify 4,000 workers in the Port of Halifax, Canada. So when an employee is banned from a site, this change cascades to every site networked with the central system.

Unisys has also worked with the Canadian Air Transport Security Authority (CATSA) to supply, integrate and manage a new identification management solution, using fingerprint and iris biometric technology to confirm the identities of airport workers throughout Canada. The Restricted Area Identification Card (RAIC) system enhances aviation security by verifying the identities of airport workers via biometrics and ensuring that only those workers with security clearance can enter restricted areas. It also allows CATSA to instantly update the security clearance status of all 100,000 airport workers across the country.

Both deployments illustrate the commercial benefits of using biometric technology to identify workers and ensure anyone with criminal intentions is prevented from entering a closed area. There has been considerable work undertaken to impress upon the public the wider benefits of this technology, in particular by developing a more people-centric approach to identity management and governance. Stronger, robust authentication is crucial in a joined-up world where information is shared. In order to improve quality of life and increase prosperity on an individual basis it is necessary to identify 'Mr Smith' the person rather than 'Mr Smith' a member of the population. The implications are far ranging; for instance, a known terrorist should be very afraid of the potential of people centric security. National identity credentialing provides better services to those who need it and very few places to hide for those who try.

Developments in biometric technology continue to push boundaries and provide fertile ground for innovation. The main challenge will be to achieve a zero False Acceptance Rate (FAR). While automation allows for greater efficiency, quick manual checks should also be made to ensure that an unauthorised person has not managed to fool the system. Nevertheless, advances in biometric technology are moving ahead at a swift pace. Project IRIS (Iris Recognition Immigration System) was introduced four years ago to provide fast and secure automated clearance through the UK immigration control for certain categories of regular travellers using biometric technology. The system stores and verifies the iris patterns of qualifying travellers, giving watertight confirmation of their identity when they arrive in the UK. It is now considered antiquated, in comparison to the latest Glance and Go iris technology, which enables people to pass through border checkpoints more swiftly and get assured while 'on the move'. Investment in biometrics is also driving research and development and expansion into new markets, such as home access and aged care services. The most significant applications will combine multiple biometric solutions with other security or identity measures, such as radio frequency identification (RFID) and smartcard technology. In any real-life application it should be heeded that the most effective approach to security is a holistic one, which assesses all possible security risks, internal and external.

" THE PUBLIC'S WILLINGNESS TO EMBRACE BIOMETRICS IS DRIVEN BY AN INHERENT EXPECTATION THAT PEOPLE SHOULD HAVE THE FREEDOM TO TRADE ONLINE AND ACROSS BORDERS WHILST ENJOYING ABSOLUTE SECURITY AND PROTECTION. "

The main barrier to the adoption and advancement of biometric technology is public readiness. As organisations reach out to the public to address their concerns we will increasingly see the application of this technology to enhance people's privacy, convenience and choice in all areas of life. As responsible messages are conveyed to highlight that privacy and security aren't mutually exclusive ideals, we could actually see people wondering how they ever managed to mitigate risk without robust authentication; in the same way that we have come to depend upon mobile phones and email. Technology has empowered organisations to choose the right combination of solutions to meet their security needs. Biometrics will undoubtedly play an increasingly significant role in the security solutions of government and industry seeking to take a holistic approach to identity management.

For further information email: Neil.Fisher1@gb.unisys.com.

Where are ID Credentials and Biometrics heading?

By Tony Seymour, MD, Seymour Consulting

The importance of Biometrics in the ever changing world of ID Cards is not in doubt these days. If you want to go abroad, show your driving licence, use a gym or library, book a hotel room or access your office and use your PC then the chances are that you will have an ID card. You might even have one per application, but that's a different story! This brief paper brings together a number of initiatives, reports etc. that are discussing the benefits of using biometrics and id credentials. References to the reports etc. are identified.

Originally, in the early days, ID cards were simple hand written documents which were manually entered to prove authenticity. Over time systems such as magnetic stripes and bar codes replaced manual methods, so that you could quickly swipe your own card to prove who you were. Recent developments have meant that using non-contact RFID technology can determine your status from a (short) distance. RFID technology is now used in the passports of many countries of the world.

So, it is clear that ID cards are an essential part of everyday life, and that we would not be able to have the flexibility and freedom that we currently do without the simplicity of ID cards.

Where is it all heading? In science fiction stories and TV, see SPOOKS in the UK, it often seems that some kind of biometric data is necessary to enter top secret locations. Fingerprint or a retina will be cloned so that they can pretend to be someone who they are not. Films show a laser device which scans your eyes, a pad that scans your palm and even a voice activated security system. Is this all science fiction?

In 1892, Sir Francis Galton published a detailed statistical model of fingerprint analysis and identification and encouraged its use in forensic science in his book Finger Prints, so fingerprints used for identification have been around a long time. One of the problems with the use of biometric information as a form of ID or access is the environmental effect on the data received. For example, poor lighting can greatly affect the image received from a facial recognition system, and fingerprints can be distorted by pressure or rotation.

Significantly the use and collection of biometric data is growing, with the United States, Japan and Australia at the forefront of biometric data collection. In Japan automatic teller machines (ATMs) now routinely use palm vein detection as part of a wider authentication scheme, and this has been very successful at reducing theft.

Of course, with any technology which is able to identify an individual, there are security concerns. The use of biometric information is seen by some as an infringement of rights, and others claim that it opens up a whole new area for identity theft, one which it will be difficult to protect against if the criminals can come up with a convincing way to "clone" an identity. Even so, the use of biometric and physical information continues to gain acceptance.

Additionally Governments worldwide are increasingly calling for powerful multi-purpose ID credentials that will cost-effectively maintain the highest levels of security while addressing secondary objectives related to more rapid processing, facility access control and e-government services.

What is Biometrics?

Biometrics is the automated recognition of individuals based on their behavioural and biological characteristics. It is a tool for establishing confidence that one is dealing with individuals who are already known (or not known)—and consequently that they belong to a group with certain rights (or to a group to be denied certain privileges). It relies on the presumption that individuals are physically and behaviourally distinctive in a number of ways. (Ref 2)

Biometric systems are used increasingly to recognize individuals and regulate access to physical spaces, information, services, and to other rights or benefits, including the ability to cross international borders.

The motivations for using biometrics are diverse and often overlap. They include improving the convenience and efficiency of routine access transactions, reducing fraud, and enhancing public safety and national security.

Overview

Over 60 countries have implemented machine-readable passports that store biometric data - facial image and, in some cases, a fingerprint - to verify identity at the border. However, there is still little or no actual use of automated biometric checks against the templates on the passport. Verification is still performed by the border guard, sometimes using the photograph from the passport chip instead of the printed image. (Ref 7)

Some countries have used, and are planning to use, biometrics for voter registration in the run-up to elections in order to prevent election fraud. These have generated a lot of press coverage both for and against its use, as there are concerns about privacy and the possibility of extending rather than reducing corruption. The European Commission, [Ref 6], says "opportunities for manipulation of personal data, mismanagement in public affairs and electoral fraud may actually increase with the computerization".

Commercial organisations, including banks, are now increasingly using biometrics for building access control, and to support authentication at remote and unsupervised locations.

UK Government ID cards

The situation regarding the UK citizen ID card with the cancellation of the ID Card programme and eventual repeal of the ID Card Act, and also the cancellation of participation in the EAC (Extended Access Control) Biometric Passports is in disarray and is currently affecting sensible discussion of the wider identity and authentication issues. With the repeal of the ID Card Act, these issues are likely to move from the Identity & Passport Service (IPS) to the new UK Office of Cyber Security (OCS). The UK OCS has a strong link to the US OCS.

However even with this very unsatisfactory situation, the UK Government is now having to face up to real authentication challenges. The main initiative is the ICT Strategy for shared services across government departments, local government and extending to suppliers. (Ref 1)

The UK Government's plan is to deliver an environment where citizens, businesses and government can enjoy the full benefits of Government information systems with confidence in their security, integrity and availability. All public sector ICT systems will incorporate information assurance from design through to implementation and disposal

The UK Government's main driver is to save money. Authentication and federation are considered a "key dependency" and solutions were being considered for implementation this year. This is a major challenge and organisations like the British Business Federation Authority (BBFA) expect a broker and a PKI bridge to result eventually. The government departments that are leading this initiative are health, defence and police departments. However with a new government having recently being elected, the ICT strategy is currently being revised. Spending plans are being reduced, but although there will inevitably be a change to the previous strategy, it is likely that information assurance will still occupy an important position.

Identity Credential Initiatives

STORK (Secure idenTity acrOss boRders linked)

The aim of the **STORK** project is to establish a European eID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID.

Thus in the future, you should be able to start a company, get your tax refund, or obtain your university papers without physical presence; all you will need to access these services is to enter your personal data using your national eID, and the STORK platform will obtain the required guarantee (authentication) from your government.

STORK planned to launch 5 pilot projects in 2010.
https://www.eid-stork.eu/

Kantara

The formation of Kantara Initiative is being driven by a common purpose -- to accelerate adoption of digital identity solutions by Relying Parties -- the organizations, applications and services that require identity credentials to complete an online transaction.

Kantara has a number of initiatives and programs ongoing.

http://kantarainitiative.org/confluence/display/GI/FAQ

Biometrics and Identity Credentials

One of the most secure and more reliable ways to authenticate a person's identity is to verify that person's biometrics. An individual's fingerprints, DNA, iris and retinal cell patterns, facial geometry, and heat signature are near to unique to that person. These biometric measures, if properly recorded, validated, and embedded in identity credentials that are logically bound to a single person's identity, can provide the highest degree of identity authentication, short of personal recognition.

Some identity credentials already incorporate some types of biometrics, such as fingerprints. The US Resident Alien Registration card, as well as several other immigration documents, has a fingerprint impression on the card. The identity verification and credential issuing process for the US Department of Defense (DoD) Common Access Card (CAC) includes collecting fingerprints.

A significant advantage of biometric identifiers is that they can be complex, and therefore difficult to duplicate. Duplicating someone's DNA is beyond the capabilities of most identity credential counterfeiters, even those who have access to very sophisticated equipment. Their complexity decreases considerably the possibility that biometric identifiers can be forged, and that complexity raises the cost of counterfeiting biometric identifiers tremendously. Using several biometric identifiers is both costly and time-consuming, but they can identify an individual with greater levels of assurance than any other type of identifier.

Some of the challenges of authenticating identity credentials are:

Multiple ID credentials

Many identity credential systems have been designed according to the "one person, one credential" principle. Ideally, a subject should only have a single identity credential issued by a specific system. Some identity credential systems do allow a single subject to have more than one identity credential issued by the same system. However, multiple

credentials issued by the same credentialing authority are redundant at best and potentially dangerous at worst.

Role-based ID credentials

Role-based identity credentials identify the role that a person is performing, not necessarily the person who is performing the role. For example, a radar operator on a ship may, during the time they are operating radar, use a role-based credential for the use of the radar operator to indicate that the radar operator duties have been performed, or that they have been performed properly.

Role-based credential systems assume that the people who use them are authorised to do so. The radar operator, for example, may be on an access control list to use the credential. The credential access systems may be designed so that the radar operator must use a personal identity credential, to gain access to the role-based credential.

Auditing identity credential use and validity

As well as a credentialing authority issuing credentials, and determining which of those credentials are valid and in use, the authority must determine if the subjects to which they were issued are still authorised to have them. Credentialing authorities should conduct periodic audits of their credential records to eliminate expired or invalid credentials

Problems with Biometrics

Biometrics combined with their use in ID cards have been seen by many as the ultimate way of providing ID credentials for the many applications that would benefit from their use.

However there remain a number of issues with biometrics, including: spoofing, masquerading, privacy, disaster recovery and restitution, storing reference biometrics, performance and storage and interoperability.

A recent study, Biometric Recognition: Challenges and Opportunities by the National Research Council has raised the issue of whether biometrics is essentially fit for purpose. (Ref 2)

A number of questions persist, however, about the effectiveness of biometric systems as security or surveillance mechanisms, their usability and manageability, appropriateness in widely varying contexts, social impacts, effects on privacy, and legal and policy implications.

Some of the principal conclusions of this study are shown below:

- Human recognition systems are inherently probabilistic, and hence inherently fallible. The chance of error can be made small but not eliminated.
- The scientific basis of biometrics needs strengthening particularly as biometric technologies and systems are deployed in systems of national importance.
- Biometric systems should be designed and evaluated relative to their specific intended purposes and contexts rather than generically. Their effectiveness depends as much on the social context as it does on the underlying technology, operational environment, systems engineering, and testing regimes.
- The field of biometrics would benefit from more rigorous and comprehensive approaches to systems development, evaluation, and interpretation. Presumptions and burdens of proof arising from biometric recognition should be based on solid, peer-reviewed studies of the performance of biometric recognition mechanisms.

Conclusions

Whilst the nirvana of biometrics on ID cards providing the ultimate proof of an individual's authenticity is something that governments, vendors, integrators would like to believe, there is now a solid body of evidence that suggests that this is not the case.

Far more research is required into the whole area of the usage of biometrics and Id credentials in order to provide confidence to the users of these systems. To ignore this and pretend there is not an issue is potentially to bring the whole area of biometrics into disrepute and ultimately widespread failure. Biometrics and ID credentials would then be heading nowhere.

References

1) BBFA : http://www.federatedbusiness.org/
2) Biometric Recognition: Challenges and Opportunities by the National Research Council : http://www.nap.edu/catalog/12720.html
3) NIST Special Publication 800-103 An Ontology of Identity Credentials Part1 : Background and Formulation : http://csrc.nist.gov/publications/drafts/sp800-103-draft.pdf
4) Kantara : http://kantarainitiative.org/confluence/display/GI/FAQ
5) National Strategy for Trusted Identities in Cyberspace : http://www.dhs.gov/xlibrary/assets/ns_tic.pdf
6) M. Adolph, 'Biometrics and Standards', ITU-T Technology Watch Report, December 2009. http://www.itu.int/ITU-T/techwatch/reports.html
7) Biometrics Update – Payment Council, May 2010

Biometrics and Multi-Application Cards

A Review of Select Applications, Programs, and Trends for the Future

By Mary Collins, Consultant, International Biometric Group (IBG)

With the increasingly global adoption of biometrics in electronic passports, many countries now have a secure way to verify their citizens' identities. The potential to leverage existing infrastructures, along with public acceptance of identity technologies in other applications, has sparked the attention of businesses and government agencies. The concept of a secure, biometrically-enabled multi-application card useable for a wide range of functions is of great interest because of the benefits it may afford deployers and users.

Typical Applications for Biometrically-Enabled Smart Cards

Multi-purpose cards are most often considered for access control, consumer ID, and civil ID applications

Access control is identifying or verifying the identity of individuals entering or leaving an area, typically a building or room, at a given time. Biometrics are used to complement or replace authentication mechanisms such as keys, tokens, and badges. The basic logic of biometric authentication is highly compelling in this environment, as keys and badges are easily shared without being traceable to the actual user, while biometrics cannot be shared without the complicity of an enrolled user. The use of a biometric creates an audit trail that is difficult to repudiate.

Consumer ID is the use of biometrics to identify or verify the identity of individuals conducting in-person or remote transactions for goods or services. The biometric is used to complement or replace authentication mechanisms such as presenting cards and photo identification, PINs, or signatures. In consumer ID applications, biometrics (most commonly fingerprint technology) are used to authorize payment for transactions from pre-funded accounts, to authorize payment from existing credit and checking accounts, or to verify identity to accept a check.

Major retailers, particularly grocers, in the Southern and Western U.S. have adopted these solutions, though there remain only a limited number of such deployments today. Many of these are focused on check cashing applications as opposed to payment authorization. Fingerprint is the dominant technology in this space, followed by voice recognition (implemented as a remote solution) and vein recognition, which has found considerable traction in ATM applications in Japan.

Civil ID is the use of biometrics to identify or verify the identity of individuals in their interaction with government agencies for the purposes of card issuance, voting, immigration or travel, social services, or employment background checks. Biometrics are used to complement or replace authentication methods such as document provision, signature recognition, and manual photograph inspection.

Several distinct applications are classified as Civil ID:

- ***Voter registration and authentication***. Biometrics are used to ensure that an individual cannot register to vote multiple times and to ensure that the individual casting a vote is the same individual who initially registered. For example, a registered voter card system was implemented in Uganda to verify voter identities and prevent duplicate registrations during the national elections. This fingerprint and face recognition system was one of the first such large scale deployments in Africa.

- ***Application for and receipt of government entitlements or benefits.*** A number of U.S. states – NY, CA, AZ, CT, and TX, among others – have made fingerprint imaging a requirement of registration for welfare and other types of public aid. Many of these multi-million dollar

programs were implemented in the early to mid-90's, and are designed to detect and deter duplicate benefits recipients. These systems have, by and large, been deemed successful. Internationally, biometric programs designed to streamline or legitimize government benefits issuance are in place in South Africa, the Philippines, and in various locations in Latin America. Each program has enrolled millions of citizens and many are expected to grow into the tens of millions.

- ***International travel and immigration-related activities.*** Driven by post-9/11 legislation and international interests, biometric technology will be used to facilitate border entry and exit for citizens and visitors, for passport and visa issuance and processing, and to verify the identity of refugees in their interaction with government bodies. Examples of this usage include implementation of biometrics to facilitate customs clearing in international airports in the U.S., Canada, and Israel; Guatemala's passport registration program, which eliminates duplicate issuance and facilitates lost passport replacement; the Netherlands' program by which asylum-seekers are verified against card-based biometric data; the European Union Schengen region's Visa Information System program, which ties the capture of biometrics to visa applications to deter "visa shopping;" and US-VISIT, which states that all machine readable travel documents must contain biometric identifiers, and all ports of entry must have equipment capable of reading these identifiers.

- ***Drivers' license or identification card issuance.*** Biometrics are used in license and identification issuance programs to ensure that duplicate identities are not created and to enable transactional functionality. Dozens of jurisdictions have implemented or plan to implement these identification programs, including Illinois, Georgia, and West Virginia; Argentina, El Salvador, Panama, Bolivia, Argentina, Nigeria; and states in India and China.

Select Multi-Application Card Programs

The most well-known multi-application card programs are in Asia. Malaysia's MyKad card, launched in 2001 was the first major smart identity card for use in multiple government applications. The MyKad contains biometric information (fingerprints and a face image), health information, and can act as a driver's license and passport. It is also used for electronic payments in low value, high volume transactions as well as for public transit and at ATMs.

Similarly, Hong Kong's Octopus card functions as an identification card, driver's license, and library card. It powers many of the country's payment systems and can be used for transportation, parking, at retail outlets, and self-service machines. Octopus cards also provide access at a growing number of residential and commercial buildings, and support various functions in schools. Octopus plans to export its solutions in system implementation and operations support to other countries, with initial deployments in the Netherlands and Dubai.

Despite the business case and interest in deploying smart cards able to support multiple applications across civil and consumer ID, few programs have taken off in Western countries where privacy concerns are a particular issue. For example, the UK planned to implement a national ID card for all its citizens with pilot programs and initial rollouts in late 2009. The card, which contained biometric information, was also intended to function as a secure travel document for travel within the EU. The UK National Identity Card scheme was recently scrapped in its entirety due to privacy concerns of the new administration.

On a smaller scale in the U.S., the Texas Health and Human Services Commission expressed interest in rolling out a universal services card to combine its four major program areas: Medicaid, Temporary Assistance for Needy Families, Food Stamps, and Women Infants and Children, each of which currently use a separate form or card for service delivery. Despite initial plans for a biometrically-enabled smart card solution, biometrics were removed for cost and public perception reasons.

Virtually none of the existing multi-application card programs are exploiting biometrics in current operations. Though biometric information is stored on the Hong Kong Octopus cards, it is not currently used for verification on a transactional basis. Many current smart card programs are being deployed, however, in a forward-looking manner such that biometrics may be incorporated using peripheral devices in the future when attitudes may change.

The biometric technologies best suited for use in multi-application card programs are AFIS, face recognition, and fingerprint, with iris recognition having some potential in day-forward deployments. The first two technologies are most capable of performing large-scale 1:N identification, with AFIS having an advantage in accuracy and scalability and face recognition having an advantage in cost and speed. Fingerprint is most likely to be used in transactional verification, anticipated to be a major component of many civil ID applications.

Trends for the Future

Multi-Application Card Growth Driversand Enablers

Both developed and developing countries, in an effort to improve services and strengthen the government's ability to interact with its citizens, are exploring the use of cards to enable various services. Issuance of multifunctional government services cards, capable of carrying information such as employment status, emergency medical information, and citizenship status, is under consideration in multiple countries across the globe. Because of the transactional elements involved, as well as potentially sensitive data, the use of a biometric to secure access to cards will increase. The South Africa model, in which biometrics are used to facilitate benefits issuance and prevent government abuse, is

extensible to a range of countries. A resistance to card-based identification programs may limit initial multi-application deployments in Western countries, although some have begun to assess the potential viability of such programs.

Of the various applications of biometrically-enabled smart cards, international border control has the highest growth potential, as countries have a compelling interest to control movement across their borders, and individuals have an expectation that processing will be rapid. Growth in this sector will be driven by the various situations in which strong authentication and singular identification of citizens is a necessity. Certain elements are more likely to grow in the U.S., Canada, and Europe, while others will find greater acceptance in Asia, South America, and developing countries, where privacy concerns are less commonplace and the need to implement identification schemes more pressing.

The availability of high-capacity AFIS systems is a key component of growth in this sector. AFIS technology is the only technology realistically capable of providing the 1:N identification necessary to establish exclusive identities, although for cost and process flow reasons jurisdictions may prefer to implement face recognition technology for less robust 1:N functions. Improvements in the technology have decreased search time and increased accuracy, such that systems will become increasingly deployable in challenging environments.

Synergies between smart cards and biometrics may facilitate use of biometrics in multi-application cards. One of the challenges of breaking into the retail market is the need to implement and integrate a biometric infrastructure, including acquisition devices and backend processing systems. Smart cards can store biometric data and verify that the card belongs to the cardholder, the primary problem faced in retail applications. Though there are some impediments to the near-term implementation of a smart card infrastructure in the U.S., the development of a smart card / biometric infrastructure in global markets is a stronger possibility.

Multi-Application Card Growth Inhibitors

It is possible that much of the growth in multi-application systems will occur outside of the U.S., Canada, Europe, and Australia. These regions have shown a general suspicion of, and occasional hostility to, extensive government-centered data collection and usage, particularly with regard to biometrics. Since many biometric identification applications are only meaningful if data is stored in a database for the purposes of 1:N matching, the potential for abuse or misuse is present. These privacy concerns are not shared as strongly outside of Western democracies, although it cannot be ruled out that resistance to government-centered systems will spread to Asia and the developing world. Subsequent to 9/11 these fears are counterbalanced by a perceived need for increased security; however, Western governments may adopt a minimalist interpretation of biometric system operations and not implement the type of pervasive systems envisioned in many jurisdictions.

Because of typical project scale, the involvement of multiple stakeholders, and the need to interface with external information systems, sales and implementation cycles for multi-application card programs are quite long. The imposing logistics of enrollment, card issuance, and identification may also inhibit the growth of certain types of biometrically-enabled applications.

Similarly, complexity of deployment is also a factor in consumer ID applications, which require devices to be deployed and integrated with current payment systems. The integration of biometrics with existing systems may be complex and proprietary to individual retailers. In-person transactions also require training of enrollers, daily operators, and users.

High-profile failures in initial MRTD applications may have generated a strongly negative impression of all related biometric solutions. Issues related to accuracy, standardization, and interoperability, many of which have not been adequately addressed in the biometric industry in particular, may cause systems to perform poorly when deployed in difficult transactional settings (as is proposed in most border crossing applications, for example). Many applications, including those already mandated and under serious consideration, vastly overestimate the functionality that biometrics can provide, incorrectly assuming that the technology is capable of addressing all issues related to identity and authentication.

General lack of education and familiarization with biometrics can also be an inhibitor in some multi-application card programs. Within any population are users who may not be technologically savvy. Some of these users may resist new technologies and only warily adopt them when more traditional alternatives are phased out. Concerns over personal privacy, safety, and hygiene – whether founded or unfounded – can limit the potential customer base for applications which are generally opt-in and thus lack the force of law or necessity that can support other applications.

Despite some remaining barriers for multi-application cards, successes of existing programs and cultivating trust in program overseers will contribute to an increase in future deployments. Resistance to biometrics and large scale deployments is compounded by the enhanced potential for scope creep when considering multi-application cards. Card functions and benefits must be clearly defined. Supervisory agents will need to establish trust in any multi-application program to gain public approval and widespread adoption.

For further information please visit www.biometricgroup.com

Global Enterprise Technologies Corp.
230 Third Ave., Waltham, MA 02451 USA
T: +1 781 890 6700
F: +1 781 890 6320
www.getgroup.com

GET. Faster

The new eP600 from GET Group is the fastest retransfer printer ever introduced for personalizing ICAO compliant ePassports. With high print resolution, fully automatic book processing, and biometric interface, the **eP600** continues the Toppan legend of state-of-the-art printers for both centralized and decentralized passport issuance.

GET. Into the future

Biometric Systems in Civil Applications

By Daniel Poder, Software Development Manager, Biometric & Web Systems and Dr Mohamed Lazzouni, Senior Vice President, Engineering and CTO, L-1 Identity Solutions

Introduction

In today's society many benefits are tied to a person's identity. The continued steady increase of the human population and high mobility, have placed identity at the center of commerce and security in today's world. Identity management requires managing new challenges and providing citizens with benefits. These benefits include the ability to cross international borders, vote in elections, and receive government services and welfare, etc. The ability to accurately identify a person's identity assists both the agency providing the service as well as the person receiving it. Evidence of this is seen by agencies spending considerable funds to prevent the misuse of their system. In the last 10 years, civil identification has adopted a tool that is more readily available than ever before to aid in managing identity – Biometric technology.

Definition

a) Biometric technology

Biometric technology can be viewed as the automated identification of a person by way of physiological and/or behavioral traits. These traits can include: fingerprint, iris, face, and a host of others. Over the past decade significant advances have been made in the accuracy of biometric algorithms as well as the overall performance of large scale biometric systems. Along with performance improvements, the general decrease in hardware cost has allowed biometric systems to become a viable tool for civil applications.

b) Biometric systems

i) Introduction

Biometric systems can add security to large scale identification systems which include vetting and enrolling an identity as well as issuing an identity document and then using it in a specific context. Biometric systems are now relied upon to guarantee that an authentic and unique identity is used for transactions requiring a high level of trust and security. Biometric systems have taken the lead in detecting and preventing many types of identity misuse. Consider a typical motor vehicle licensing authority. The goal of this agency is to provide a driver's license to individuals who have proven capable of operating a motor vehicle. However in the United States a driver's license has become a de facto proof of identity (it plays the role of a National Identity in other countries). Because of this, issuing agencies are under increasing pressure to ensure that the issued credential is given to the citizen whose identity has been vetted with great care and trust.

ii) Design goals, types of identity attacks and system examples

Identification systems used in civil applications require scalability, availability, reliability, real-time and ease of use. There are also two primary functional requirements the biometric system must prevent: identity theft and duplicate identities.

Identity theft:

Identity theft typically occurs when one person claims the identity of another. A biometric system can help detect this type of misuse by comparing the associated biometric trait (typically a facial image) of each new issuance of a driver's license to all the previous issuances of the license. The correct images associated with correct individual can be found, and if an impostor attempts to assume that identity, his/her image will fail to match the images of the genuine identity. In this manner, the biometric system guarantees the ideal of 'one person-one record'. Without a biometric system to automatically compare images there is a great chance that an impostor can assume a stolen identity and use it to gain illegal access to legitimate benefits and documents.

Duplicate identities:

Another common type of identity attack is when a person attempts to establish multiple identities. This occurs when a person uses a fake name(s) to get a fraudulent license. In some cases people will have several aliases with several credentials. They can then use these fake identities for a variety of criminal schemes, many of them involving financial and banking fraud. A biometric system can help detect this type of system misuse by comparing each newly captured facial image against the entire set of facial images in the licensing database. These searches require increased computing power and algorithm performance because each newly captured facial image is compared against millions of other facial images.

iii) Privacy vs. security

Biometric systems require judicious design and careful use. Privacy is a corner stone of open societies. The right against unsanctioned invasion of an individual or group privacy by entities ranging from corporations to government is protected

by law and must be respected. The need for higher security to protect an individual's life, assets and liberties is equally important. Biometric systems in their design and deployment must respect privacy and security requirements and find a working formula to manage conflicting requirements. The public's perception of biometric systems tends to be that of criminal and forensic applications. Certain types of biometric traits are closely related to law enforcement such as fingerprints and DNA. Civil biometric applications can be designed and deployed to enhance customer service experience by being accurate, user friendly and real-time. For example when a police investigator uses a biometric system to collect latent fingerprints at a crime scene it is acceptable to wait hours or even days to get back a list of potential matches, this would be unacceptable for a civil identification application, such as opening a bank account or obtaining a driver's license.

The balancing act between privacy and security, accuracy and customer service has been an area of interest for the last 10 years and has seen significant progress, where vendors of biometric systems and agencies using them have worked hand-in-hand taking into consideration a variety of items, such as the number of transactions per day, agency staffing, biometric system performance, and performance to come upon with optimal solutions.

One of the notable advances in civil identification applications using biometric systems has been the use of self service. In civil biometric applications the general public will be interacting with the system. Devices and systems collecting biometric data have become so intelligent that multiple modalities can be captured without the use of an operator. Fingerprint collection devices offer real-time feedback to guarantee the collection of fingerprints with very high quality and without retake. Face capture has become so widely ubiquitous that self-capture is the norm in collecting portraits. Iris capture can now be achieved 'on the move'. The search and matching technology is abstracted and the results are returned in a user-friendly manner. To make the system successful, biometric system designers have taken great strides towards making users comfortable with using the systems. Often people associate fingerprinting with law enforcement and criminal activity. In motor vehicle offices across the United States, tens of thousands of people are processed daily using facial recognition systems – doing so with great ease and efficiency.

iv) Best practices

Although the demand for multi-modal biometric solutions is on the rise, civil identification applications continue to require the face as the biometric modality. The reason for that is quite simple. Portraits have been captured historically and are available abundantly. Systems designed to use Facial Recognition follow certain best practices which allow for optimal system performance. A solution can typically be broken down into the following elements:

Frontend biometric capture:

This is where a person's facial image and demographic information are gathered.

Backend biometric processing:

This is where the captured data is stored and processed. It is here that images are turned into biometric templates and compared against other previously stored records.

Frontend biometric capture: Starting with the capture application it is imperative to get high quality images. Better image quality can reduce false matches and poor template generation. To meet this objective it is recommended to follow certain image quality standards. One such standard is provided by ICAO (International Civil Aviation Organization).

As a matter of best practice for facial recognition systems the following is true of most captured facial images:

> Neutral expression, no glasses, direct frontal view, no more than a 10 degree head tilt off vertical axis, image resolution to exceed 90 pixels between the eyes, and lastly no obscuring of facial features by hair, hats, patches, etc… Following these image quality rules allows for the best possible template generation and thus a higher accuracy in matching.
> The capture application should have automatic software checks in place for each of these image quality values. By doing this at the capture station it allows operators to retake pictures until a valid image is obtained.

Backend biometric processing: Once an image is captured and the applicant claims this is the first time he is being entered in the system, the facial image is sent to the backend biometric application for storage as well as comparison against all other images in the system. This identification process determines if the person is already in the biometric system possibly under a different identity. This is where duplicate issuances are found. If any other images have a high enough similarity score, the backend system makes the resultant matches and newly acquired image available for manual review by human operators.

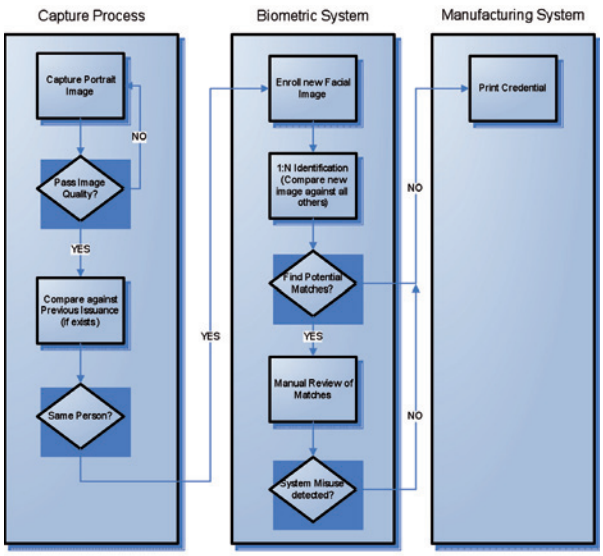
If instead the person claims this is a renewal of a previous credential, the capture application can perform another action prior to sending the image to the backend biometric system. It is desirable for the capture application to retrieve the most recent facial image on file for the identity the person is claiming. The capture application can then do a 1:1 facial image comparison. At this time the capture application presents both images along with the low similarity score for operator review. This can greatly reduce attempted identity theft while also keeping the integrity of the data in the backend biometric system as clean as possible.

v) Biometric systems driving issuance and personalization of ID documents

In a civil identification application such as Voter ID systems or Driver's licensing systems, it is highly recommended to closely couple the biometric solution to the ID document issuance and personalization process. As an example, if a facial image is captured and no potential matches are found by the biometric solution, the biometric application can inform the manufacturing process to print this credential. Similarly if the biometric solution finds potential matches, the credential should be put in a pending state by the issuance and personalization process until a final resolution is achieved by a human operator. If the operator determines system misuse has occurred the biometric solution will deny the credential from being manufactured.

> By following this practice, fraudulent credentials caught by the system do not make it out of the issuance and personalization processing. This significantly reduces the number of fraudulent credentials in circulation.

This in turn gives increased confidence in the validity of credentials which are in general circulation. Below is a high level workflow design of this process.



vi) ID document issuance topologies before and after the use of biometric systems

Instant issuance before a fully integrated biometric authentication in the vetting of identity

In the case of instant issuance without the use of biometric authentication, a driver's licensing system captures the process in a manner similar to the generic solution described above but with one major difference – there is no backend manufacturing process. The credential is physically printed during the capture process and handed to the applicant as soon as the capture process completes. Historically this was a very common practice and in many areas applicants expect to get their credential the same day. The issue with this type of system is the biometric identification happens after the applicant has already left the capture location with their credential. If afterwards, the biometric system finds potential matches and a human operator determines system misuse, the invalid credential is already out in general circulation. This increases the workload for the agency because they have to start the process of revoking the already issued credential as well as tracking down the individual. This also lowers the confidence of outside agencies/consumers of the validity of credentials in general circulation.

Instant issuance after a fully integrated biometric authentication in the vetting of identity

In this case, the driver's licensing system performs the biometric identification in sequence with the capture process. By doing this the agency is able to issue credentials at the capture location while still ensuring the integrity of the identities in their system. In order to do real-time biometric identifications from the capture application it is imperative the biometric solution's hardware and algorithms are sized appropriately to meet performance expectations. For example if an identification takes 10 seconds to return results to the capture application, and 50 capture locations all issue identification requests simultaneously to the biometric solution, the biometric hardware needs to be scaled appropriately to handle this load so that each capture station gets results back in a timely fashion. If the hardware is not scaled appropriately, during peak volumes the capture process can be delayed by several minutes per applicant.

> " In examining the usefulness of biometric systems in conjunction with large scale civil applications it is clear there are numerous benefits."

Conclusion and summary

In examining the usefulness of biometric systems in conjunction with large scale civil applications it is clear there are numerous benefits. Agencies looking to add a civil biometric capability to their existing systems need to carefully design how the biometric solution will be integrated. There is no doubt that the biometric system will help ensure data integrity but the cost-to-benefit ratio needs to be evaluated at design time. As a person's identity becomes increasingly tied to societal privileges, as well as financial benefits, the ability to prevent various types of identity theft becomes imperative. Issuing agencies will be increasingly interested in enhancing their solutions to meet this demand and properly designed biometric systems can be a key tool in combating this issue.

For more information please visit www.l1id.com.

New Frontiers

By Sue Coutin,
Marketing Manager, Datastrip

The evolution of a 'borderless world' has created new challenges for governments in protecting their citizens against crime and terrorist attack. Peter Hradek from Datastrip looks at how next generation portable biometric devices are being used as part of effective identity management solutions to help combat such threats.

Increasing globalisation of economies and the growth in the movement of the world's population have helped erode traditional notions of countries and nation states and instead has led to the formation of the concept of a 'borderless world'.

Technological trends, particularly in internet communication, have also helped strengthen the connection between individuals, businesses and society and economies – leading to the erosion of 'virtual borders'.

The UK's newly released National Security Strategy points out that faster and cheaper travel, the flow of ideas and capital around the world has ensured that distances between people and events are becoming less relevant.

"All those are positive changes, empowering individuals and creating new opportunities for businesses, organisations and whole nations," says the strategy.

Schengen agreement

The signing of the Schengen Agreement by 25 EU countries has also contributed to the concept of the 'borderless world' as the agreement allows people travelling in the countries who have signed the agreement to move freely with no border controls.

Whether a passport or an EU approved national identity card is required for identity checks done at airports, hotels, or by police, depends on national rules and varies between countries. Occasionally, regular border controls are used between Schengen countries.

Complex dichotomy

The increasingly complex international landscape and blurring of traditional notions of borders has come at a high price for many countries that have seen an increase in cross border crime, smuggling, drugs and piracy as a result.

This has created a complex dichotomy for governments who are keen to promote and encourage the free movement of people while at the same time recognise the importance of protecting their citizens against the threat of crime and terrorist attack.

Eurojust the EU body that was set up to provide a coordinated response against international crime reported that the number of cross border investigations brought to its attention increased by 15 per cent in just one year in 2009.

A co-ordinated investigation led by Eurojust helped dismantle a criminal network of a hundred Albanian-speaking criminals who were involved in cocaine trafficking across Belgium, France, Germany, Italy and the Netherland.

It resulted in the seizure of substantial amounts of cannabis as well as firearms and heroin.

Organised crime involving fraud, the trade in illegal drugs and illegal weapons, illegal immigration and human trafficking (especially of women and children), is increasing across the world. Where those activities thrive, they threaten lives and legitimate livelihoods; undermine and corrupt economies, societies and governments; help cause or exacerbate state failure, in some cases leading to civil war and violent conflict; and can directly or indirectly support terrorism.

Those phenomena are not new, but they are taking new forms and exploiting new opportunities, including revolutionary changes in technology and communications, and increased global movements of goods, people and ideas.

Identity theft

One of the biggest casualties of the move towards a 'borderless world' is the increase in identity fraud, money laundering and counterfeiting – activities that are often carried out to fund terrorist activities.

Identity fraud is big business in countries including the US which has stepped up its efforts towards combating the crime by setting up an identity theft task force.

Two years ago, the US authorities followed the discovery of a gang of eleven criminals who stole more than 40 million credit and debit card numbers before selling the information. They hacked into the computer systems of several major US retailers and installed software to access account details and passwords.

The market for faked passports and other forged documents has also grown significantly over the past 20 years as criminals are increasingly exploiting the readily available technology to help them create supposedly authentic documents that can withstand the scrutiny of security checks at borders.

Three years' ago, the Metropolitan Police uncovered the largest haul of fake passports ever found in the UK. More than 1,800 fake passports with a street value of at least £1 million were discovered in a flat in north London.

Fake passports for at least 12 countries were found stuffed into a wardrobe, cupboard and briefcase. Among the documents were 200 fake UK passports which are often considered by counterfeiters as too difficult to make.

Other passports were Finnish, Portuguese, Korean, Latvian, Slovenian, Albanian, Danish, Greek, Italian, Belgian and French.

Also found was a mass of hi-tech equipment including printers, scanners, two computers and various false immigration stamps.

Thousands of blank passport personal information pages as well as blank driving licence cards were also discovered. When officers entered the property, a counterfeit driving licence was being printed in the back bedroom.

Identity management

With so many people moving about in this new increasingly free flowing 'borderless world', one of the key challenges for authorities is verifying the identities of individuals as there is still currently no one single internationally recognised form of identification.

Despite the move by many countries to adopt e-passports in an attempt to tighten up on security, many countries still do not consider the passport as being the main form of identity. Imagine the dilemma for port and airport staff across the world when having to check identities of people travelling from multiple countries – all carrying different forms of identity?

Further adding to the challenges, is the fact that the majority of mainland countries have multiple entry points with no formal borders and often no manned entry checkpoints.

Any checks that are carried out vary from country to country and involve staff from a number of different agencies, again depending on the country. This could vary from customs and border control staff, to police and in some cases military officials.

Technology solutions

This potential risk to a country's national security cannot be underestimated; governments and security agencies have been increasingly looking towards technology to provide effective identity management solutions. One of the greatest advancements is in the area of mobile electronic readers which help address many of the issues we've already outlined in relation to the threats brought about by a 'borderless world.'

These increasingly sophisticated and technological advanced portable readers are designed to be carried by the guard or border agent, so they go wherever the guard or border agent needs them.

In countries where there are no formal borders – the mobile readers allow guards or border agents to make random checks of vehicles or sea vessels and to be more flexible in the way they carry out physical checks.

The need for the technology to be interoperable between different agencies is also a must as it has been proved that a joined up approach to identity management is the most effective way of combating crime and security threats. This means that information about a person's identity can be shared among agencies.

Mobile readers

Counter terrorism officers at UK ports and airports are using mobile document readers to conduct identity checks on passengers. The new devices can scan passports and are able to check identity details against data held on the Police National Computer (PNC) – a database of information on known criminals that is maintained and held by police forces in the UK.

Det Supt Paul Everett from the Association of Chief Police Officers (ACPO) Terrorism and Allied Matters (TAM) liaison unit said that the technology had increased the effectiveness of his officers and that he would support more widespread introduction.

Use of the readers has resulted in a number of significant arrests, including one individual who had an outstanding international warrant out against him for murder.

Similar devices are also being used for homeland security, military and commercial applications in Europe, the Middle East, Africa, India and North America.

Mobile readers are specifically designed to read and validate a variety of documents, not just passports and to assist with the identification of individuals. This ensures that they are truly an international solution and could help provide some consistency in the way documents are checked and verified in each country.

Across the globe, security officials have recognised multimodal biometrics as the way forward for the positive identification of individuals. Currently, multimodal solutions - a combination of facial, fingerprint, iris, palm or voice recognition - show the greatest potential in military, law enforcement, Homeland Security and commercial physical access applications.

Multimodal systems which can combine facial, iris and fingerprint biometric identification, help agencies overcome the limitations of using just one biometric as their ID verification tool.

For example, integrating two or more types of biometric recognition and verification systems allows facilities to comply with stringent programs such as the Homeland Security Presidential Directive 12 (HSPD-12) and the Federal Information Processing Standard 201 (FIPS 201).

Agencies have more opportunities to verify IDs and secure their facilities when multimodal systems are integrated with mobile devices. When housed in rugged hardware, handheld biometric terminals can go virtually anywhere to provide instant, on-the-spot ID verification. The technology also allows for on-the-stop enrolment and rapid checking of identities in seconds.

Essential requirements

Mobile readers have to fulfil certain robust criteria in order for them to be used effectively in a 'borderless world'.

It is essential that they are rugged and flexible in construction. Due to the fact they can be used at less formal entry points that might be remote, they must be designed to withstand harsh weather conditions and unpredictable movements.

Long battery life is also a must as devices that need to be frequently charged create unnecessary down time and could compromise security checks. Mobile readers allow staff to work in multiple locations – sometimes often remote locations where there are no formal borders and so long battery life is a must in any device.

Manufacturers of mobile readers have worked hard to ensure they are field tested to enable them to operate effectively in mission critical environments and also meet tough government verification requirements for biometric equipments.

" Even though the mobile readers are now using the most advanced technology, they are designed to be easy to operate by a whole host of different personnel. "

It is also essential for mobile readers to be able to be easily integrated within existing identity management systems.

Even though the mobile readers are now using the most advanced technology, they are designed to be easy to operate by a whole host of different personnel. It is essential that staff are able to process documents quickly and efficiently in order to cope with high through-puts of travellers as well as ensure that the travelling experience is a pleasant one. There is little point in promoting free borders and the increase of people traffic from country to country if any checks that are done are time-consuming and slow down passenger movement.

Another important benefit is that because the readers are compact and lightweight they are considered relatively unobtrusive to passengers who are used to seeing 'hand held' devices in their every day lives.

One of the criticism of old methods of identity management is that they were cumbersome and too intrusive, making travellers feel uncomfortable and feel that they were being unnecessarily exposed to heavy handed verification techniques.

Future challenges

It is essential that manufacturers continue to develop mobile reader technology in order to keep pace with ever rapid advancements in other technologies which will only increase over the next ten years. Continued research and development and collaborations with other companies will therefore be vital in the years to come.

As these new forms of technology develop and become increasingly more sophisticated then criminals will continue to find new ways of staying one step ahead for their own financial gain – something we need to be constantly mindful of if the technology is to remain as effective.

With countries predicting that the flow of people traffic will only increase in the years to come, then we should be under no illusions about the challenges and issues that lie ahead as we continue to move towards a truly 'borderless world'.

For further information please ontact: www.datastrip.com or sue.coutin@datastrip.com

Enhancing Security through Mobile Biometrics

By Tiffany Christoffers, Corporate Marketing Manager, Cross Match Technologies, Inc.

Identity verification is of the utmost importance for national and commercial entities seeking to provide secure environments. Biometric-based systems are a popular choice and are currently in use worldwide to aid in the verification of individuals' identities entering and exiting secure areas. By capturing and verifying physical traits, such as fingerprints, iris and facial images, organizations are enhancing the security of their facilities by ensuring that only authorized individuals gain access.

Traditionally, biometric systems are stationary or portable; allowing little mobility for users. However, as biometric technology evolves, the capture systems are becoming smaller, lighter and faster. With the introduction of mobile biometric capture systems, users are integrating them into existing security schemes, adding ease of use and flexibility to their programs.

US-VISIT and TWIC go mobile

Mobile biometric identification devices have been used for many different applications during the past several years. Law enforcement agencies, the Federal Bureau of Investigation (FBI) and other national organizations have been using mobile systems to allow personnel to capture fingerprints, iris scans and facial images in the field. Applications include secured location access control, and identity verification for employees and contractors.

One such initiative is the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program. This United States Department of Homeland Security (DHS) immigration and border management program involves the collection and analysis of fingerprints and other biometric data, which is compared against a national database to track illegal immigrants, criminals and terrorists.

The Transportation Worker Identification Credential (TWIC) program is a complementary initiative of the Transportation Security Administration and the US Coast Guard. The program provides a tamper-resistant biometric credential to maritime workers requiring unescorted access to secure areas or port facilities and vessels regulated under the Maritime Transportation Security Act of 2002. To obtain a TWIC, an individual must provide biographic and biometric information including fingerprints and a digital photograph.

The DHS and the Coast Guard are incorporating mobile biometric devices into these programs to help screen visitors to the U.S. and to verify workers' identities. "New technologies are being evaluated to help improve the accuracy and efficiency of government biometric collection," states Mike Oehler, Vice President Product Management, Mobile Biometrics at Cross Match. "Multimodal mobile technologies play an important role in that evaluation process."

One such example is the ongoing partnership between the Coast Guard and US-VISIT officials to deploy mobile biometric systems on Coast Guard cutters operating in the Mona Pass between the Dominican Republic and Puerto Rico—helping to address the challenges of coastal security. The mobile biometric devices have allowed the Coast Guard to identify hundreds of undocumented aliens, some of whom were already enrolled in the US-VISIT program as prior felons or immigration violators who have previously encountered government authorities.

The integrated mobile solutions are not only being used for identity management but also for credential verification. Rugged, multimodal handheld solutions extend existing physical access control systems, allowing ports to utilize these devices when authenticating TWIC cards. "Wireless solutions that read contact and contactless smart ID cards and contain barcode and fingerprint scanners allow users to read most forms of identification used in port environments," explains

Oehler, "The flexibility of the mobile systems allows users to easily secure both interior and exterior environments."

A pilot program worth the RISC

Parallel to the US-VISIT and TWIC programs, the FBI has created the Repository for Individuals of Special Concern (RISC). It provides law enforcement and partnering agencies with rapid identification services to quickly assess the threat level of an encountered individual. The system uses a minimum of two or a maximum of ten fingerprint images (flat or rolled) to conduct an automated search against a limited population of approximately two million records, including: wanted persons, sex offender registry subjects, and known or suspected terrorists.

To best leverage this pilot program, the FBI is evaluating mobile biometric systems to access the backend data in RISC. "Mobile biometric devices deliver the flexibility, reliability and speed that personnel demand" says Oehler. "These solutions are ideal for federal investigation and special forces programs, in addition to homeland security initiatives and federal employee identification programs."

Mobile data sharing

The US-VISIT, TWIC and RISC programs have one thing in common—biometric data to be shared among partner organizations. For instance, if the Department of Defense (DOD) wants field personnel to be able to search DHS, FBI and DOD databases, the mobile devices must be compatible. Oehler explains, "The biometric data captured from a given mobile device is not necessarily readable from another system. A variety of data formats, templates and images add to the complexity of ensuring compatibility among mobile systems."

> " As mobile device standards continue to evolve, selecting products that meet those standards will be invaluable to customers. "

This issue is being addressed at a national level, as just in 2009, the Advisory Policy Board (APB) to the FBI's Criminal Justice Information Services Division (CJIS) approved a request to develop a set of guidance principles for mobile biometric capture systems. The resulting Mobile ID Device Best Practice Recommendations (BPR) address the capture of fingerprint, iris and facial images in generic use cases for law enforcement, defense and homeland security applications. "Mobile device features, software capabilities, communication and security protocols are addressed in the BPR document," notes Oehler.

Currently, biometric solution vendors are working to help ensure interoperability among agencies using mobile devices. For instance, systems are entering the market that support standards-based EFT files for images and M1 for templates. Image quality is being addressed through the implementation of FBI Appendix F-certified optical fingerprint scanners and Mobile ID BPR Subject Acquisition Profiles (SAP) as high as level 45. Advances like these help improve the interoperability, quality and accuracy of mobile biometric capture systems.

Choosing a mobile solution

When considering mobile biometric solutions, it is important to select a system that combines the necessary features for your security installation. For instance, integrated units are readily available that combine fingerprint capture with smart card authentication in an easy-to-use, handheld device. Such units also enable users to synchronize data with one another to rapidly verify subjects' identities in the field.

As mobile device standards continue to evolve, selecting products that meet those standards will be invaluable to customers. "Choosing standards-based mobile systems is key because it provides users with an upgrade path to interoperability with other agencies," explains Oehler. "Many biometric solution vendors are committed to bringing mobile devices to market that will address customers' changing needs. Selecting a biometric solution vendor that embraces this philosophy will help ensure a successful mobile deployment that will remain an integral part of your security program for years to come."

For further information please visit www.crossmatch.com

New Identity Cards:
providing security, confidentiality and opening the door to eServices

By Eric Billiaert, Marketing Communications Director, Government Programs, Gemalto

A hallmark of citizenship and cohesion

The right to identify citizens, but also the duty to protect their identity, are perfect examples of the responsibilities that come with a State's right of sovereignty.

The secure documents issued by government authorities for just this purpose not only allow states to identify their citizens but also to distinguish them from foreign nationals, who may, for whatever political or economic reasons, seek to fraudulently benefit from rights reserved to citizens of that particular state.

These documents enable the citizen to exercise their rights and responsibilities. Clearly, document theft and fraud are sources of social injustice as the community may inadvertently allocate resources to an ill-intentioned individual feigning another person's identity, thus depriving the genuine citizen of that to which he or she is legally entitled.

The most important requirement is therefore the inviolability of issued documents. It is quite clearly the reason why states are now modernising their national identity documents to move over to highly-secure documents incorporating all the very latest secure printing innovations.

A means of guaranteeing the security and protection of citizens' data in a digital world

The number of digital exchanges has increased exponentially over the last 10 years, from 100 million to 30 billion private or professional emails. Ease of use goes hand-in-hand with the general public's perception of the relative fragility of electronic media.

The absence of "written proof" and eye witnesses, which is characteristic of electronic modes of exchange, very quickly led to the identification of a requirement to guarantee the identity of the issuer or the receiver.

Since 1997, the design, production, and deployment of Secure Electronic National Identity Cards, more generally known as "e-ID Cards", have been seeking to meet just that requirement.

The idea of an electronic identity card which is both physically valid and valid for digital use is fast becoming a reality

Furthermore, the electronic format of such ID cards means that, in addition to being used for electronic signature applications, they are also ideally suited to be employed for other uses such as access cards to grant the holder access to company infrastructures or secure locations, as well as social security cards and in some countries, drivers licenses, healthcare cards, "Pass cards" for transport services, payment cards or even bank cards.

The main objectives of states today presented to our industry are:

- Build a modern, secure civil state on which public services and administrations can confidently rely on and are sustainable.
- Modernise identity documents in order to help actively combat document fraud and increase levels of trust at both national and international levels.
- Ensure compliance with international identity and travel document standards.
- Help to bring about decentralisation and strengthen the bond between public services and citizens.
- Provide a shared and future-proof platform for the creation of identity documents and the delivery of public services for all government authorities.
- Lay the foundations for a modern, digital economy.
- Provide citizens with a guarantee that their data is protected and can be exchanged in confidence (e-Identity or identity on/for the net).

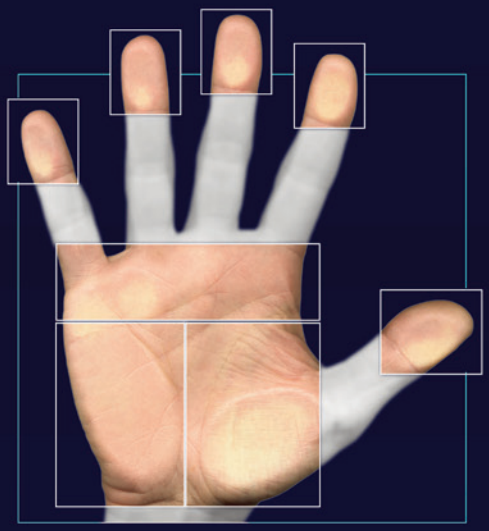
How does it work and what does it do?

The smart card (microprocessor) is considered to be the most secure means of authentication, making it possible both to prevent identity fraud and protect citizen's personal data in an effective way. It is the media of choice for granting access

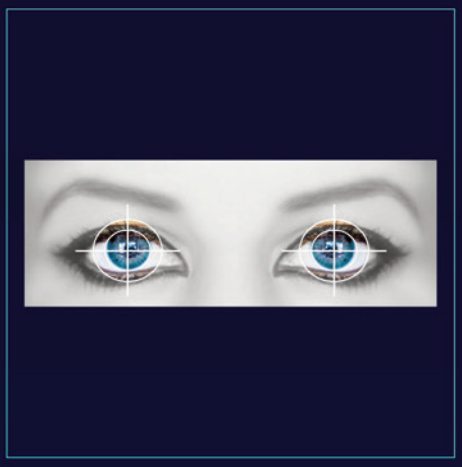
CROSSMATCH®
TECHNOLOGIES

Protecting People, Property and Privacy

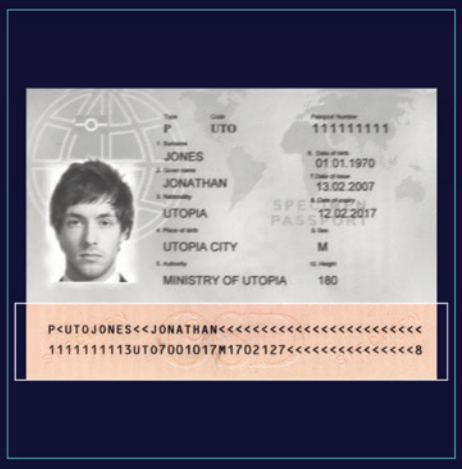
Multimodal Identity Management Solutions



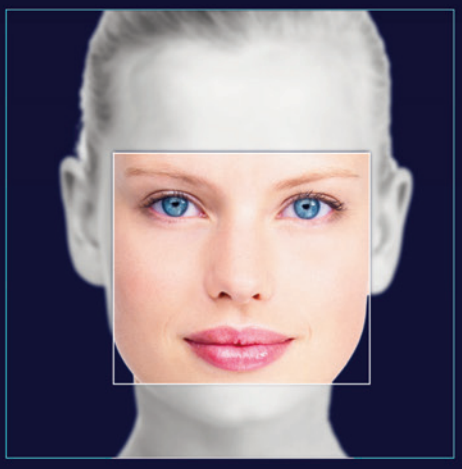
LSCAN®



iSCAN™



DSCAN®



FSCAN™

www.crossmatch.com

Cross Match Technologies

Corporate Headquarters, USA:
(Sales North & South America)
sales@crossmatch.com

German Operations:
(Sales EMEA, Asia & Pacific)
international-sales@crossmatch.com

to e-Government applications. It can also be used as a means of hosting a range of other applications (e-payment, e-purse, digital signature, authentication, identification, travel card, etc.). This potential to provide a range of different services on a single format means a number of uses can be brought together in the most ergonomic way possible, thereby transforming a simple State identity card into a card which is of genuine use to the citizen, granting them access to the widest possible range of State services.

Thanks to the chip incorporated into it, the e-ID card is now able to serve three distinct functions. Identification, authentication and signature.

The first function of the identity card is identification of the holder. The e-ID provides exactly the same information as the traditional identity card but this information is also stored on the chip. The e-ID can therefore be used for two different forms of identification:

- Visual, face-to-face identification: using the information visible on the card,

- Automatic identification: by acquisition of the data stored on the chip. This sort of identification can be performed remotely over the internet.

Identification alone (whether it is visual or automatic) does not allow us to be certain that the applicant is the person he/she is claiming to be. To be sure of this, we need authentication. This is where the second function of the chip on the e-ID card comes into play: card holder authentication. This is a new function that was not physically present on old identity cards. The electronic chip contains a digital certificate of authentication which can "electronically" prove the identity of the cardholder. Authentication offers a better level of security than identification as it requires the user to be in possession of the e-ID and to know the corresponding PIN code.

The third function is also an addition to what was offered by the conventional identity card. A second certificate, located on the chip of the electronic card, allows for an authentic electronic signature to be applied to electronic documents.

After entering his/her e-ID card, the citizen can then confirm his/her approval in a window which will then generate a unique document signature. Every year, each citizen fills out a large number of administrative forms that all have to go through a more or less time-consuming identification process. This process, currently a reality at many different counters throughout the country, usually involves the following steps:

- The identity of the applicant has to be checked by the civil servant,

- Data has to be transcribed or encoded,
- The applicant has to sign his/her application.

Using e-ID cards, these operations can all be performed in seconds.

The quality, the reliability and the perceived value of an identity card (in this instance the polycarbonate Swedish ID card) all help to build confidence and facilitate adoption.

The quality, the reliability and the perceived value of an identity card (in this instance the polycarbonate Swedish ID card) all help to build confidence and facilitate adoption.

Uses:
- Local administrations
- Police stations
- Post offices
- Banks
- Social sector
- Vehicle or equipment rental services
- Transport (in Estonia)
- Healthcare and hospitals (Malta, Belgium, Italy, etc.).

Benefits:
- Saving time: identification processes are carried out much more quickly and efficiently, even in an over-the-counter setting
- In terms of physical identity checks, the visual inspections are carried out in the same way as with a traditional card. Border control personnel can check the photo saved to the smart card
- Quality and consistency of information gathered: a strong decrease in the number of errors/inaccuracies in coding
- Reduction in the number of errors in data entry
- Economy and ecology: a reduction in the amount of paper used means less archiving is necessary

Online access control

These applications are carried out remotely and therefore require a computer, a card reader and an internet connection.
As for physical access control, it is important to be able to

filter access for certain internet sites, applications and databases.

Applications:
- Internet sites requiring specific access control (teleworking, restricted user groups, secure emails)
- Restricted access for minors to certain sites with sensitive content (forums, online gambling)
- Access to databases and their online files

Benefits:
- Simplification and ease of use: reduction in the number of identification methods used
- Increased security on the internet
- Better protection of minors

Identification and authentication on the internet

The authentication element of e-ID is probably the component that offers the most potential, by offering the capacity for digital signature. Electronic authentication is something that is to set to revolutionise our lives as citizens. All official documents that previously had to be approved with a manual signature will now all be able to be authenticated with an electronic signature.

Uses:
- Online declarations (tax declarations, VAT declarations, and police)
- Remote signature of contracts
- eVoting
- Remote justice (remote submission of testimony, submission of decrees, remote access to verdicts rendered)
- e-Commerce (purchase of tickets for sporting events, remote public auctions)
- Professional certification cards (lawyers, solicitors)

Benefits:
- Significant time savings: the user doesn't have to travel to the point of delivery
- Cost savings: travel costs, postal costs
- Widespread availability: service available 24/7, regardless of the user's location
- Ecology: reduction in the amount of paper used

The deployment of these digital documents provides real services and benefits to citizens and companies in terms of their day-to-day interaction with local or national administration.

Our observations clearly show that e-ID has become a real catalyst for the success of e-Government, particularly in countries where communication goes hand in hand with the modernisation of relations with citizens and businesses. Demonstrating that e-ID is an efficient tool for the exercising and protection of citizens' rights.

Two key factors are strongly associated with the success of this project: citizens' confidence in and adoption of these secure documents. The card ensures secure access to digital files and protects the citizen's personal data and all their virtual administrative documents against any form of intrusion. In addition to covering more conventional needs in terms of physical security and use of the internet, such as e-Commerce, payments, online taxes, and secure access to administrative files, new areas of application where such solutions can be used to benefit citizens and businesses are gradually being opened up as part of various pilot schemes.

Examples of these applications are:

- Monitoring, treatment history and prevention in healthcare, (Belgium, France, Germany, Algeria, Portugal…)
- Children's aid (Belgian Kids-ID)
- Computer ticketing or e-Ticketing, "Swipe Cards" as a way of regular billing for local transport subscriptions (Estonia, Spain, Belgium)
- Secure purchasing for the extended enterprise (France, Belgium, Italy, etc.)

"Police on web" is one of the 600 eServices with strong authentication available in Belgium. Your bike is stolen? Graffiti on your wall? Don't move, use the web.
100% of the population has an e-ID card in the country early 2010. Belgian citizens can now identify themselves and report crimes to the federal police via the Internet. The process saves significant time compared to the traditional lengthy process of reporting crimes at police stations, which takes an average of two hours. The scheme is part of the Belgian government's plan to simplify the country's administrative processes.

- Access cards for access to private or public secure locations or public car parks

- Application links with digital verification of roles and powers of authorization for use in the international exchange of confidential government data (Austria, Belgium, Europol, EuroJust, etc)

- Electronic vote, e-participation and free internet access for citizens attending debates and deliberation sessions of local authorities (Estonia, Belgium, France, Spain (Barcelona), etc.)

What are the main concerns of citizens?

Our studies (Gemalto 2007-2009) systematically show a higher degree of sensitivity when it comes to "proximity" services in areas such as social services, healthcare, finance and education, followed by transport and access to public leisure services as a second phase. The success of online tax declarations has been concrete and spectacular right across Europe. In addition to this, in countries where the most progress has been made, we can see a strong synergy between policies at both national and local level (Austria, Belgium, Estonia, Portugal, Sweden, etc).

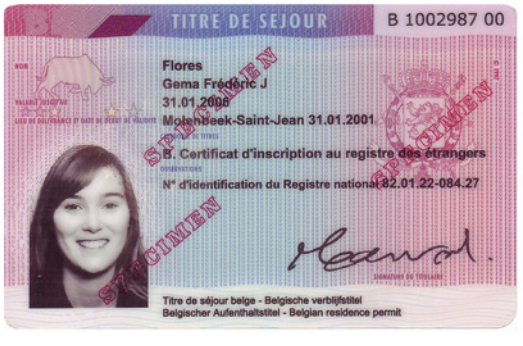
For further information please visit www.gemalto.com

Gemalto's credentials to comment

Gemalto's credentials to discuss these issues are based on the fact that we have delivered the core technical solution to 15 out of 25 national electronic ID implement ations currently operating around the world.

We believe that this gives us an excellent insight into the technology, its applications and the social context of its use.

" Thanks to the chip incorporated into it, the e-ID card is now able to serve three distinct functions. Identification, authentication and signature. "



Greater than the Sum of their Parts:

Multi-technology ID cards deliver advanced functionality, efficiency and security

By Stephen Price-Francis, Vice President of Marketing, LaserCard Corporation

Evidence is mounting that multi-technology, multi-functional credentials are the wave of the future when it comes to secure ID.

Source: **LaserCard** Corporation

Heightened security concerns, high traffic border crossings, and a growing requirement for streamlined government services delivery are just some of the factors driving this trend. Governments and national organizations are increasingly viewing upcoming ID programs as an opportunity to increase efficiency as well as protect and ensure the identity of the holder. This has given rise to projects calling for powerful multi-purpose ID credentials that operate on multiple additional levels, maintaining the highest levels of security while addressing additional objectives such as entry to secure facilities, faster border crossing, or access to health and social services. All this on a single card platform!

While ID card decision makers are becoming knowledgeable about the benefits delivered by a more robust, sophisticated credential, the many available technology options present a somewhat confusing array of choices regarding the design, manufacture and combination of elements.

While the concept of a multi-functional card may conjure elegant simplicity, the reality is complex. Considerable design, technical and manufacturing expertise must be employed to ensure that the end result conforms to international standards in terms of size, security, functionality and durability. Nevertheless, such cards are ultimately a more cost-effective, efficient option than single-purpose credentials and enable the program specifiers to ensure a uniformly high standard of security across all functions.

Technology combinations for advanced functionality

The delivery of a broad range of functions on a credit card-sized credential generally requires the use of two or more different technologies. These can include integrated circuit (IC) chips, radio frequency identification (RFID) tags, or optical security media. Thus an ID card might include an optical security media for storage of data and visual authentication, and a contactless chip for facility access.

Typically, secure credentials employ one of three principal categories of advanced technology: IC chips, RFID tags, or optical security media.

IC chips, commonly used in Smart Cards, verify and control transactions between the credential and its reader and may contain such information as biometric, personal, or account data that individuals need to effect transactions. RFID tags are primarily used to facilitate fairly long-range wireless communication of a serial or file number to a reader. This is useful, for example, to notify a land border inspection system of a card's impending arrival (with the assumption that the

rightful holder is also present) so as to facilitate the border crossing. Optical security media is a tamperproof, highly counterfeit-resistant visual and physical security feature that can also store unalterable data related to the credential holder, such as a high resolution facial image and biometrics. While each of these secure ID technologies lends unique capabilities to an ID credential, a combination of technologies on a single card can deliver far greater value than any one solution.

Six layers of security

Multi-functional ID documents should incorporate a layered system of security, with six layers providing the optimum protection.

- Layer 1: front line, eye readable and tactile security features that can be verified with the unaided eye of the examiner and by touch.
- Layer 2: security features that the examining officer can validate with the use of simple hand held tools i.e. magnifier (loupe) or ultraviolet light source.
- Layer 3: security features that are created during the personalization process, including a 'swipe' of the machine-readable zone.
- Layer 4: biometrics, securely stored in the document, which will then scientifically match the biometric to the bearer when a 'one to one' live verification is made using an appropriate reader.
- Layer 5: a technology that allows instant access to a database that would contain biographical images and data (a 'one to many' identification check), and would also check the document and bearer against a watch list.
- Layer 6: security features and/or codes that can only be authenticated with forensic equipment. These forensic features for all intents and purposes would be virtually impossible for most counterfeiters to replicate.

This multi-layered approach provides some serious hurdles for counterfeiters to overcome. They can no longer simply scan, reprint and mass-produce credentials. It will be very difficult for them to replicate these documents and have them be creditable at any level. A multi-technology credential is often the best choice for this approach.

Combining identity technologies for multi-purpose ID cards

Multiple identity technologies currently co-exist in cards issued under major ID programs, including Italy's Carabinieri (national police force), Saudi Arabia's national ID card program, and the new US Green Card. Some states in India uses a hybrid vehicle registration card that contains optical media for data storage in combination with a chip for transactions related to vehicle registration fees. In this paper we discuss several real-world examples of multi-technology card use.

Two types of IC chip—contact and contactless—are widely used by governments and businesses in Europe and Asia for transactions that include financial and healthcare information. Cards with contact chips are physically inserted into an electronic reader, while contactless chip cards, which contain a chip and an antenna, must be passed within close range of a reader to exchange information via radio waves. Both types of smart card can be encrypted and further protected via PIN or biometrics. While IC chips alone provide secure machine authentication and transaction control, the addition of another secure ID technology, such as optical security media, enhances the card's visual and physical security, also delivering a forensic level authentication capability. It also greatly increases counterfeit resistance, and provides back-up to the chip's data should it fail for any reason.

Fraud prevention

People from all walks of life are routinely asked to provide proof of identity at border crossings, airports, medical facilities, and even office buildings. Paper credentials are very obviously an invitation to forgery, but even seemingly sophisticated ID cards are also vulnerable to counterfeiters. Today, advances in counterfeiting techniques make it more difficult to visually authenticate an individual's identity credential.

This is evidenced by a recent US Government Accountability Office report regarding the US-Mexico Border Crossing Cards. Although these relatively advanced credentials included state-of-the-art security printing and other features, they were found to be unduly vulnerable to counterfeiting. Contrast this with the US Permanent Resident Card (Green Card) issued by the Department of Homeland Security, which has been described as 'putting mass counterfeiters out of business'. The Green Card features highly durable polycarbonate construction, tamper-proof optical security media, a Personalized Embedded HologramHD , ultra-high resolution overt, covert and forensic security patterns, and visual security elements that are extremely difficult to reproduce and can be verified with a simple inspection tool.

In the case of multi-functional cards, the requirement for security, durability and advanced manufacture and design is all the greater.

Next generation US Green Card

The new version of the US Green Card, introduced in May, 2010, is the world's first implementation of a combined

optical security media and Radio Frequency Identification (RFID) tag on a single card. RFID tags are widely used in manufacturing and retail to associate an object with an identification code. When an RFID tag passes within range of a reader, it transmits data via radio waves.

The RFID component of the Green Card facilitates more efficient transition through land border checkpoints and complies with the Western Hemisphere Travel Initiative (WHTI) requirements. The Green Card's graphic design also includes high resolution offset printing and other visual security features. Innovations that further enhance security include ultra high resolution security artwork, resolved at up to 25,000 dots per inch - beyond the capability of technologies typically used by counterfeiters - and a large, high contrast, high resolution tamperproof cardholder image laser etched onto the optical security media (LaserCard's Personalized Embedded HologramHDTM).

The next-gen Green Cards, front and back:

Front of card: *" The next-generation U.S. Green Card features a host of high resolution offset printing, artwork, and other visual security features"*

Back of card *(featuring optical security media stripe: "A large, high resolution, tamperproof cardholder image is laser etched onto the optical security media using LaserCard's Personalized Embedded HologramHDTM) technology.*

The new Green Card has recently been judged the world's leading government ID card in terms of technology and user utility in a new report by analyst firm Frost & Sullivan, who describe the card as setting a new standard for international ID programs.

By providing an additional 'visual' security layer, these cards help bridge the gap created when technology resources such as card readers or network connections are unavailable, while significantly reinforcing visual card inspection wherever it is required.

Combining RFID tags and optical media in a single credential balances two superficially conflicting objectives: the convenience of efficient and speedy movement through a secure access point, and the overarching requirement of the highest levels of credential security.

Optical security media differs from IC chips and RFID tags in that it does not employ electronic memory. Optical security media is immune to the risk of electromagnetic erasure or interference. In addition, optical media delivers substantial data capacity: sufficient to allow storage of high resolution, original biometric images such as fingerprints, irises, and facial characteristics, plus the cardholder's photograph, name, digitized signature, date of birth and registration number. The data storage capabilities of optical media open the potential for portability of detailed biometric data within single credentials, across a variety of recognition systems, and international interoperability. This information cannot be erased or fraudulently altered and private data is protected from viewing by any authority other than the issuer.

" THE DESIRE OF GOVERNMENTS AND BUSINESSES TO ACHIEVE MULTIPLE PURPOSE CREDENTIALS CONTINUES TO GATHER MOMENTUM. "

THE CHALLENGES

The desire of governments and businesses to achieve multiple purpose credentials continues to gather momentum. However, the integration of multiple technologies and compliance with international standards that limit the size and thickness of ID credentials present several complex challenges. To ensure the effectiveness of a multi- purpose ID credential, a card manufacturer must take into account materials science, ISO and other standards, durability, and a host of technical and structural considerations.

In their search for multi-purpose secure ID solutions, government agencies and commercial enterprises are turning to manufacturers capable of developing secure ID credentials that integrate proven technologies in a single platform. IC chips, RFID tags and optical security media each offer unique advantages. By combining two or more of these technologies on a single card, issuers can realize the cost, efficiency and security benefits inherent in a multi-application credential that verifies identity, accesses e-government services, facilitates efficient border crossings and physical access, all with the highest level of counterfeit resistance.

For further information please visit www.lasercard.com.

Complexity of Corporate Identity Smartcards in the Enterprise

....And how to avoid the most common pitfalls

By Terry Gold, Vice President, US Sales, idOnDemand Inc.

Societies in general have struggled with the concept of identity throughout time. They have mainly relied on the government to assign, issue, and produce a form of "identifier" for individuals to use to verify their identity to gain access to various services. Non-government organizations have relied on government as well in this effort, so individuals can prove their identity to access their services or gain memberships to them. Over the years, Identity has evolved from simple paper-based forms, to incorporate PhotoID, and have undergone various modifications to make them more sophisticated to resist forgery efforts and maintain a level of trust in society. As they have done so, the private industry has increasingly relied on this model.

This model had worked reasonably well, to the extent that there was a longstanding sense of complacency to accept whatever form of government issued Identification was available; no standards bodies, consortiums, or working groups to influence what was being produced or accepted. However, the age of electronic information, its pervasive use and availability, and the requirement for the exchange and collaboration of such information has fundamentally changed how organizations, consumers, industry and government think about Identity. At the core, the effort and challenge has become to balance the creation, issuance, process and usage so that it is both secure and pervasively usable with ease.

There is a direct correlation in our perceived ability to achieve this, and how much "trust" we place in the overall viability of the process. There has been a clear evolution in the concept of proof of identity, the level of access granted as a result of providing such proof, as well as where and how such access can be applied. Society, organizations and individuals increasingly demand fewer credentials that can be used across a broader variety of applications, while expecting the trust to be there as well.

The smartcard has emerged as an increasingly obvious (and uniquely) platform to address these challenges due to its wide variety of uses, security model, opportunity for consolidation and portability. It is also a form factor and user experience that people are used to. However, the implementation of smartcards has proved to be very complex, coupled with many dependencies, and ultimately too expensive for most organizations. This is not to say that the cards themselves are too expensive or complex; rather the dependencies, skill sets, and project resources required are typically overwhelming to organizations and eroding the estimated return on investment. No matter how much value is placed on the smartcard, the longer the project runs without completion or realization of estimated features, its value is cannibalized by the complexity and effort.

What makes deploying smartcards so complex and are there ways to take advantage of smartcards , realize their value, and have more control over the deployment to ensure success? YES. This article will review years of large scale deployment experience, to uncover some of the most common pitfalls that are the main contributors to a project's demise, and can be avoided.

Complexity:

Before we can go into what should be avoided, perhaps a primer on why deploying smartcards is complex is appropriate. Most people that decide to implement smartcards in an organization, aren't experts with smartcards, and are under the impression that the technology associated with them is all about the card itself. Therefore, much of the preparation is focused on selecting a card based on speed, performance and capacity and as a result, underestimating the real considerations ahead. The fact is, the smartcard manufacturers have done an excellent job at building them to contain their complexity, they are all fairly comparable in terms of performance to the point where an end user will not notice, and evolving standards and the use of many of the same components in manufacturing from the same sources make most of them on par with one another – to the extent that such differentiation does not materially impact the deployment, its complexity, or its success very much - at all. The complexity comes from the following areas:

1. **Key Management:** To maintain the intended security model that is unique to smartcards, it is required that the inherent key management be deliberately executed. For example, it is best practice to not use the manufacturer's default or provided master key, generate your own, and then swap the keys on the cards at time of issuance to ensure that your security model is unique. There are many steps in doing so, none that are trivial, and if not done improperly, an entire card population can be compsimised both from a security and operational perspective. The level of knowledge, expertise, and systems required are not common and typically underestimated.
2. **Backend Dependencies:** To securely issue credentials in a manner where a user's assigned credentials can be managed effectively throughout their lifecycle with the organization, credential management software, clustered database instances, and key integration points to directories,

IDMS's, Certification Authorities, Key Management, and other systems are required. This requires intense operational focus across a variety of expertise domains to be successful.

3. **Personalization & Distribution:** Putting a card into the hands of remote users, and not just those that are internal, and dealing with replacing them when lost, is quite a different support model than the current physical security program. A user cannot just come to the building to pick up a new card. Also, printing is more complex, going from simple equipment to more specialized and from a 20 second print to nearly 6 minutes on average.
4. **Lifecycle Management:** Activation, termination, PIN resets and dealing with lost cards are al scenarios that need to be addressed. For example, if a user loses a card, CIO's do not want more help desk calls and revert back to the domain passwords (temporarily) that they were trying to get away from in the first place. These are things that need to be figured out ahead of time, and often customized into a solution.
5. **Policy, Process & People:** To take advantage of what a smartcard offers, its incorporation into an organization mandates that such future processes around issuance and usage, are complimentary to the overall goals they support. Ultimately some policies and processes will likely need to evolve.
6. **PKI:** The wisest and most experienced professionals wink and tell each other that "it is easy to set up, but hard to do it right". If it is not done right, the entire trust model along with encrypted items, can be compromised and need to start over. Doing it right is costly, but doing it wrong is even more so.
7. **Lack of Experience:** For the vast majority of organizations, a smartcard project is the first of such for everyone involved resulting in the inevitable learning process and challenges that come with it.

What is at stake?

To setup an internal infrastructure correctly, plan on spending a few hundred thousand dollars between hardware security modules (HSM's), Card Management Server setup, server hardware, Database instances, the various skill sets internally, externally and collaborate with other colleagues internally for support and integration. It gets very expensive even before buying licenses, cards or readers to then issue to a larger population. Therefore, it is important to eliminate as many items that can cause delays and failures as much as possible.

After years of focusing on large corporate rollouts, below represents pitfalls that can easily be avoid yet are the most common for impacting projects:

Focusing on the card first:
The single most common pitfall of all is an organizations's immediate reaction to start their investigation into a smartcard deployment by searching for card and subsequently basing the project activities on which card they are going to select. More times than not, this approach leads to total project failure and the organization's inability to materially use the chip on the card. Due to the numerous dependencies on the back end in terms of integration, key management, servers, and how an organization may need to unique deal with them relative to THEIR environment (current investments), it should first be investigated as to what card management software will be selected, which Certification Authority it needs to support as well as how they are going to employ key management and other critical components, prior to selecting a card to ensure that whatever card is chosen, its profile and applets are supported. Doing so in the reverse order only leaves compatibility to chance, wastes a lot of time and political capital in the process which is important for a project of this magnitude.

It is suggested to architect the backend, call out dependencies, have a clear vision of integration points, and a solid project plan prior to purchasing cards. In fact, it is advised to not even engage in a search for cards until such a time. The card management vendor will be able to clearly tell you which cards are compatible. At this point, always test the cards in a pre-production system with the CMS and respective client before committing to a specific card vendor.

Failure to clearly define goals of project and articulate them across functional teams and stakeholders:
Due to the highly technical nature of a smart card deployment, many organizations go right into technical investigation mode without first defining what features, workflows, integration points and policies need to be supported. This leads to long test cycles that often miss properly identifying the most suitable software and vendors to work with for their specific environment resulting in large obstacles to overcome later on.

Failure to review current policies and identify if new ones need to be established:
Since policy shapes process, which in turn dictate functionality and features, the impact can be large if this is overlooked at a starting point.

Failure to have cross functional executive stakeholder support:
Executives with the power to appropriate competing project resource efforts need to be involved to maintain the level of commitment to this type of project or progress can completely stall since many of the resources are shared experts. It is also critical that stakeholders resolve internal politics between groups and ensure that goals are clearly articulated and agreed.

Solution Definition:
Failure to establish policy, process, features and technology that is aligned with the goals of the initiative, makes it almost

impossible to establish an accurate solution definition that is critical to address dependencies unique to the environment (upgrades, legacy systems, anomalies in integration, etc) that are hard to change but require thought out countermeasures and the right vendor selections. It also then difficult to establish accurate project plans, resource efforts, and timelines. A proper solution definition should be completed prior to purchasing any production licenses of software or smart cards, and then validate the all assumptions through a small scale production environment. Plan to make adjustments to the solution definition, ensure vendor reviews that they can completely support these prior to scaling out for mass deployment.

Details in integration:
It is one thing for a vendor to check a box that they support integration into another application, and another to find out later that such integration in execution does not meet your specific expectations in terms of exception handling or your unique implementation of the product. Often there are many details for example of HOW a certificate on a card will get renewed. Will the user get notified, is the CMS aware, do the two versions cooperate well together so it is seamless to the end users, not just that it "integrates". Sometimes one of these (and there are typically multiple) situations delay project plans for months at a time as they often need to be resolved by multiple vendor parties and ultimately an enhancement is then required.

Lack of Standards:
Going down a proprietary path often leads to vendor lock-in, higher prices via single source models, and end of life challenges. Use open standards that are currently available to avoid costly limitations and having to consider ripping and replacing the entire infrastructure.

Attrition of personnel on core team:
The skills sets of the core components of the smartcard infrastructure eventually get finely tuned to deal with the challenges that they faces and the anomalies that present themselves moving forward. Reduction of force, transfers, or resignations prove to be highly disruptive to the entire operational team and typically will take 9 months to get a replacement to the same level again, stressing the whole team. Have a continuity plan and commitment from management upfront as to the criticality of maintain the team.

Too much focus on "convergence":
While there is value in converging identity, credentials, and processes between building and IT Security, unless the definition of convergence is clearly defined, validated that it has an operational and organizational value that is quantifiable, it is typically a large effort with little result. This should be defined and decided in the early phases. There are also various contexts of convergence based on who is asked, but the right definition is the one that is defined by the customer under careful consideration of their environment, goals, and determined value.

Failure to Identify required customizations:
Each component of the smartcard ecosystem plays a specific role and no one product can do everything. Much of the time, if some features are required, they must be developed and maintained by the customer. This could be anything from a front end, lost card workflow, temporary access or bridging binding the identity and credential for each environment (building system and then IT). Balancing what is core, verses what needs to be developed, with the right vendor to satisfy dependencies specific to your environment is the key for vendor selection and resource allocation to support it.

Lack of engaging the right partner
Whether it is a vendor or a consultant, employing the assistance of an expert that has done large scale deployments with similar goals in the past, from inception to completion will help navigate if not most, then all of the pitfalls discussed. Do not just employ an organization that has done so, but the specific people on the project that they assign is key.

Other Options:

Up until this point, a traditional in-house, deployment model has been discussed. Recently, other options have become available in a service model format. By using a service that already has the infrastructure setup and ready to use, audits completed, and lifecycle features built to avoid customizations, a great deal of time, money, and resourcing can be eliminated. Some even include the full PKI infrastructure, key management, printing, distribution, and activation. Typically, these services will require less capital up front while not requiring resources operationally and over the course of its life will be much less expensive as well.

IdOnDemand, who all came from the traditional model, have addressed the pitfalls to offer a turnkey service that is extensive and enterprise-class, but simple. A comparable 2 year project, from vendor selection through production build and card issuance, can be about half the cost and be done inside of 2 months resulting in reallocating that capital and resources to other projects that might not have otherwise been completed.

Also, traditionally, in order to reach some form or acceptable ROI, such capital required of a traditional approach would need to be spread across a large enterprise user base to have a low "per user" cost. This often made an enterprise-class smartcard deployment unobtainable. With a pay-as-you-go, per use fee, anyone who is small, or wants to start small, can have a static cost model that is low; whether it is 5 users, or 50,000.

All approaches should be investigated and considered to see which one is right for you.

For further information please visit www.idondemand.com

My Access to my Business.

Any service I can imagine, any security level I desire.
All on one chip. On the credential of my choice.
Contactless smart card technology: www.legic.com

LEGIC®
innovation in ID technology

Smart Cards and the Proposed U.S. National Strategy for Trusted Identities in Cyberspace

By Randy Vanderhoof, Executive Director, Smart Card Alliance

In May 2009, U.S. President Barack Obama announced his intention to make cybersecurity a priority for his administration with a "new comprehensive approach to securing America's digital infrastructure."

Since then, the Obama administration has taken several concrete steps to achieve that goal, creating a new Cybersecurity Directorate, appointing a Cybersecurity Coordinator to provide leadership and launching a number of initiatives ranging from education to a national response strategy for significant cybersecurity incidents.

Potentially the most far-reaching actions now underway—and certainly those of greatest import to the smart card industry—are to develop and implement a national vision and strategy for securing identities in cyberspace.

After a year of research, in May the White House released to the public for comment a draft of a *National Strategy for Trusted Identities in Cyberspace* (NSTIC).

In this paper, we will review the key elements of the NSTIC strategy and its potential impact, which in the end could extend far beyond the United States, with a special emphasis on the likely role of smart cards as the technology of choice for protecting high value identities.

The Vision

The goals of the NSTIC strategy are to ensure that identities of people, organizations and devices can be trusted on the Internet, and that they are better protected from the threats of identity theft and fraud. Simply stated, the NSTIC calls for the creation of an online environment where individuals can voluntarily choose to obtain a secure, interoperable and privacy-enhancing digital identity credential from a variety of service providers – both public and private – to authenticate themselves online for different types of transactions. The NSTIC attempts to define a Framework that provides many options for identity verification. The draft strategy includes important privacy protections and is based on a user-centric model that allows users more control of their private information. Most importantly, it acknowledges a range of authentication options depending on the specific requirements of each transaction and individual preferences.

Analysis

The NSTIC initiative correctly recognizes that there are very real problems of identity management, privacy and security in U.S. society today, and brings a much needed focus on solving the problems. Although its scope is limited to cyberspace, the Framework would also establish essential foundational elements that can help to strengthen identity, privacy and security in healthcare, social security administration, immigration reform and other programs in the physical world.

The NSTIC Framework draft is well conceived and written. To start with, it is voluntary, so no one is forced to use anything it defines. It is intentionally broad in scope, providing a wide range of trusted identity constructs and identity protection technologies. The Framework is very pragmatic and practical in its approach, because it limits the role of the federal government to being an enabler, facilitator and accelerator of the Identity Ecosystem development. There is a clear recognition that many different public and private stakeholders will be involved in working out the specifics of the Framework and ultimately, using it.

An Identity Ecosystem

The objectives of the national strategy are to be able to trust and protect online identities. To achieve this goal, it broadly defines all of the elements that would be needed to create an Identity Ecosystem, including processes, roles of different parties and types of identity protection mechanisms.

In order to have a productive national dialogue about identity, we require a common vocabulary, and one of the accomplishments of the NSTIC Framework is to define the terms necessary to discuss an Identity Ecosystem. Some key terms that are not readily obvious to people familiar with identity and access management are:

- **Identity Provider (IDP)** - Responsible for the processes associated with enrolling a subject, and establishing and maintaining the digital identity associated with an individual or a Non-Person Entity (NPE), an entity with a digital identity that acts in cyberspace but is not a human, such as organizations, hardware devices or software applications. These processes include identity vetting and proofing, as well as revocation, suspension, and recovery of the digital identity. The IDP is responsible for issuing a credential, the information object or device used during a transaction to provide evidence of the subject's identity; it may also provide linkage to authority, roles, rights, privileges and other attributes.

- **Identity Medium** - A device or object storing one or more credentials, claims or attributes related to a single subject, and in the case of a device, capable of transforming these information objects for specific uses. The identity medium is any credential, card, badge, USB, smart phone or other media, regardless of form factor, issued or authorized for identification purposes within online transactions.

- **Relying Party** - A relying party is a provider of online services to a subject. Within the ecosystem, a relying party is responsible for interacting with credential, identity and attribute providers as needed to verify parties with whom they exchange information.

The Role of Smart Cards

To start moving forward, the Framework proposes the excellent idea of using federal, state and local government and academia programs to accelerate development of the Identity Ecosystem. At the same time, it recommends leveraging existing U.S. federal government procedures, standards and technologies that are already well defined and broadly deployed.

Of particular interest to the smart card industry is that the Framework document cites this technology as an example of an identity medium suitable for high-value transactions and identities. Furthermore, it highlights smart card standards such as the Federal Information Processing Standard (FIPS) 201 and the Federal Identity, Credentialing and Access Management Roadmap. These standards and guidelines evolved in response to Homeland Security Presidential Directive (HSPD)-12, which mandated a government-wide smart card-based ID for all federal government employees and contractors, now known as the Personal Identity Verification (PIV) card. The extension of this program for government contractors is the interoperable PIV-I card. Other federal programs that leverage the standard include the First Responder Authentication Card (FRAC), Transportation Worker Identification Credential (TWIC), Common Access Card (CAC) and other identity programs.

This bodes well for the smart card industry. Every U.S. federal government employee has a smart card. Why? To provide a governmentwide identity credential that is secure, biometrics capable and ready to be used with physical access control systems as well as online for authentication, encryption and digital signatures.

The fact that the Framework, which is intentionally technology agnostic, identifies these standards and smart card technology as examples strongly indicates broad recognition that these elements provide a solid foundation for assuring high value transactions and identities in the proposed Identity Ecosystem.

In addition, the idea of starting with government programs is also favorable to the smart card industry. Private enterprise will ultimately embrace the idea of identity management as a cornerstone of best business practices; however, the federal development of standards and processes for an Identity Ecosystem will foster and accelerate greater acceptance. Combine this with the fact that the federal government is already moving ahead with smart card technology for strong authentication and high assurance identities, and you have a situation that is very favorable to the industry.

Prioritizing

The first priority should be first defining the Identity Ecosystem for the most trusted digital transactions based on an identity medium. This part of the Identity Ecosystem can have the greatest positive impact on identity, security and privacy. It is also the least developed and therefore needs the greatest attention and leadership.

Many private sector software-based initiatives, such as Open ID, are already commercially available and are suitable for lower assurance identity transactions. What is needed urgently is a way to provide individuals the opportunity to have a trusted digital identity credential that cannot be misused if stolen or misplaced, and cannot be compromised through spyware, phishing or data breaches in either individuals' own PCs or the information systems of service providers.

Using an identity medium that is independent from a PC and that can serve as a secure container for PKI digital identity certificates, biometrics and other identity protection technologies, is the only way to solve all these problems quickly. Ultimately, the identity transaction must begin with a verifiable token, managed by the Identity Provider.

Ease of Use

Ease of use is a goal of the Framework. A suggested idea to make high-value identity transactions both secure and easy to use is the familiar approach of a card and PIN as an identity medium; however, to achieve high levels of security, the card must include smart card technology to carry PKI credentials, biometrics and other security features. It could even carry multiple identities or personas for different purposes. The approach of using a card carrying PKI credentials is very easy for the user, because it provides strong digital identity protection without burdening individuals with the complexity, responsibility and risk inherent in keeping PCs free of spyware, or learning how to spot phishing attacks and hacker websites.

An Identity Ecosystem that includes smart card technology as an identity medium for high-assurance online identity transactions will provide a very strong and proven foundation for protecting identities in cyberspace in a secure, privacy sensitive way. This foundation can be put in place without reinventing the wheel. The federal government has already established a set of best practices, standards and technology solutions for smart card-based identity management and authentication that can be adapted to this initiative.

What is the advantage of using smart card technology?

A smart card provides high levels of security and privacy protection. Unlike PCs and other open systems, smart cards are designed for security and are virtually impervious to malware, forgery and other fraudulent efforts to extract information.

Smart cards can provide a secure tamperproof container for PKI digital identity credentials and biometric identifiers. In addition, they can be delivered in a familiar card format, making them both portable and easy for broad public distribution and use.

These capabilities make smart card technology ideal for protecting identities and privacy, and for preventing fraud. Smart cards are readily used online and across networks and deliver very high levels of security over the Internet.

Conclusion

Protecting identities in the online world is a global priority. The executive branch of the U.S. federal government has recognized there are very real problems in cyberspace of identity management, privacy and security, and has proposed a coherent, voluntary national strategy that acknowledges multiple levels of identity assurance and well need for commercial and governmental identity providers.

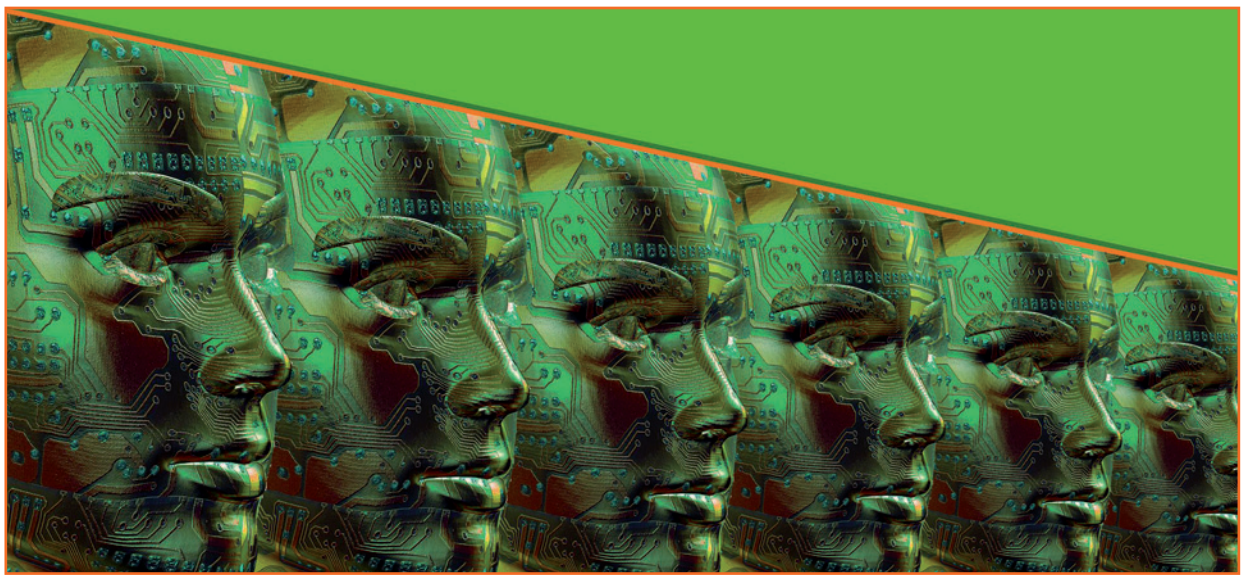
The public comment period on the draft framework is already completed. As this article goes to print, the next step is widely expected to be the publication of the approved framework document. From there, public and private stakeholders will begin examining projects that can help to build out the components of the framework, improving identity security in cyberspace over time.

Smart card technology is already the identity security technology of choice in several federal programs, which gives it a strong position to emerge as the foundation for high assurance identity authentication. As NSTIC moves ahead, the Smart Card Alliance Identity Council and its members, which include many in the government identity and authentication community, will continue to actively contribute ideas and resources to help move this very important initiative forward.

This article draws from specific comments on the NSTIC Framework draft prepared by the Healthcare and Identity Councils of the Smart Card Alliance, a U.S. non-profit public/private partnership organization whose members include healthcare providers, financial institutions, payment brands, enterprises, government users and technology providers. The Smart Card Alliance is very active in the area of identity management, security and privacy. Its diverse group of members provides a well-rounded perspective on identity issues because of the different stakeholders in the group.

More information is available at: http://www.smartcardalliance.org/pages/activities-councils-identity including the following white papers:

- Healthcare Identity Management: The Foundation for a Secure and Trusted National Health Information Network
- Assurance Levels Overview and Recommendations
- Identifiers and Authentication -- Smart Credential Choices to Protect Digital Identity
- Identity Management Systems, Smart Cards and Privacy
- Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology
- Secure Identification Systems: Building a Chain of Trust



Silos All Over Again:
The Case for Authentication Management

By Idan Shoham, Chief Technology Officer, Hitachi ID Systems, Inc.

Most medium to large organizations have a large number of applications, each with its own database of login IDs and passwords. Even as some applications are modified to leverage common platforms, such as Active Directory, which in turn can be smart-card enabled to authenticate users, other applications operate in a stand-alone fashion.

As illustrated in Figure 1, most organizations are trending towards multiple passwords:

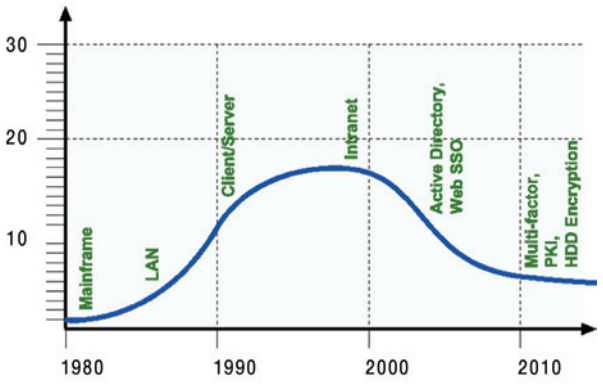


Figure 1:
Trend in the number of corporate passwords per user

Today, a typical corporate user has several credentials – one Active Directory account plus one or more of the following:

1. A LDAP directory account (i.e., other than AD).
2. An ERP account – SAP R/3, PeopleSoft, Oracle eBusiness Suite or others.
3. A mainframe login - RAC/F, ACF/2 or TopSecret.
4. A smart card or token.
5. A password or card used to unlock the encrypted hard drive on his PC.
6. One or more accounts on "cloud" applications, such as www.SalesForce.com, Ceridian, ADP or others.

Most medium to large organizations have deployed some combination of identity management, password synchronization, password reset, single sign-on or federation software. This is supposed to move the support processes for all those credentials – onboarding, support for forgotten, lost or stolen states and deactivation – out of the application silos and into a shared infrastructure.

The war against security administration inside the application has been hard fought and won (or so we thought).

Administration silos are back…

So what's new and why are administration silos a problem once again?

Organizations are now deploying a whole range of new technologies and each of them introduces its own administration and support processes. For starters, every authentication technology depends on some onboarding process, which includes activation of a given user and/or device and on a termination process, which may involve user deactivation, device deactivation, certificate revocation or reclaiming physical inventory.

In addition, each technology needs some process to support users who have a problem with login process or need to sign in from a device that does not support the technology in question. Here are some examples:

- Users with a smart card may have misplaced their card or forgotten their PIN or may need to sign into a corporate system or application from a client device that does not have a smart card reader. While card readers are getting common on company PCs and laptops, they are still pretty rare on home PCs and smart phones.
- Users with hardware tokens (one time password / OTP device) may have forgotten their PIN or misplaced their token or maybe just haven't used it in a long time and the clock on their token has drifted too far away from the clock on the authentication server.
- Organizations that want to use a biometric system to authenticate users into a computer network or just to open a door, need to consider user logins from devices without a reader or doors where a reader cannot be reasonably installed. There may also be users who cannot use the biometric in question – e.g., blind users may not be able to use

a retina scanner, amputees cannot use finger print or finger vein devices, etc. Finally, biometric samples need to be collected from every user prior to use of the system.

- Even users whose PCs are protected using full disk encryption technologies need support. They may forget the password that must be typed before their hard disk is unlocked and the operating system can be bootstrapped.

The vendors of each of these solutions have obliged their customers and generally offer both self-service and assisted-service solutions for PIN resets, key recovery, biometric enrollment, etc.

The problem with all of these solutions is that each one is specific to just one product. This means that we're back to silos – expensive and user-unfriendly. This is illustrated in Figure 2.

Figure 2: **Administrative silos: each technology comes with its own support mechanism**

Consider just three examples, all to do with security questions:

- A user enrolls a set of security questions with RSA Authentication Manager, which he can use to prove his identity in the event that he forgets his RSA token PIN.That's great - but can the same security questions be used to authenticate the user who forgot his network password?

- A user enrolls a set of security questions with a full disk encryption product, which he can use to prove his identity in the event that he forgets the password that activates his PC. He can use this to perform key recovery and get back to work, but can he use the same authentication process if he forgets the PIN to his smart card?

- A user enrolls a set of security questions with an Active Directory specific self-service password reset product. This profile information cannot be used to authenticate the same user if he has a problem with his hardware token or even with another password (e.g., RACF, SAP R/3, etc.).

When we had just passwords, the solution to these support problems was to modify applications to validate passwords against a common LDAP directory, to synchronize passwords between applications that cannot be configured to use an LDAP back end and to provide self-service password reset for users who forgot their password or locked themselves out.This had the effect of reducing the number of passwords users had to remember and enabling users to resolve their own login problems without calling the help desk.

Design principles for authentication management

Today, the same sort of solution should be extended to support all of the authentication factors that a user may have, rather than just passwords. An authentication management system should embody three core principles:

- **One application, accessible anywhere:** A single application should be accessible by users who need assistance, regardless of what authentication technology they have, what kind of problem they are having or where they are stuck. For example, a smart card user locked out of his Windows login screen because he forgot his PIN should be able to access the same system as a user with an encrypted hard disk who forgot his PC activation password and cannot boot Windows, who should be able to access the same system as a mobile user who is currently in a hotel room, but forgot the PIN to his OTP token and cannot establish a VPN connection.

- **Authenticate with one factor to manage another:**Users should be able to sign into the consolidated support application with whatever authentication factors they have and still work. For example, they should be able to answer security questions or use an OTP token or use a smart card or have a random PIN sent via SMS to their mobile phone or use a biometric. The basic assumption here is that there are many ways to authenticate a user and when a user needs help with on of them, he can still use another.

- **Integrate enrollment processes:** Where enrollment is required, all of the steps that users must go through to provide information should be merged into a single, easy-to-use process. For example, users should never be invited on one date, to one URL, to provide security questions and to another URL, at another time, to provide a biometric sample.

Scenario	Accessed from	User authenticates with	Administrative actions
Smart card PIN reset	The login screen of a PC with a card reader	Answering security questions, random PIN to mobile phone via SMS, etc.	The user chooses a new PIN for his token, which is applied to his smart card by an ActiveX component embedded in the self-service UI launched from the PC login screen.
Self-service password reset	The Windows login screen or a web browser on another PC	Answering security questions or an OTP token or a smart card, or a random PIN sent via SMS to the user's mobile phone or any combination of these.	The user chooses a new password for one or more systems and applications, despite having forgotten or locked out the current password one.
Token PIN reset	A phone call – typically this is used by mobile users, who forgot their PIN and cannot establish a VPN connection	Answering security questions or a voice biometric.	The user chooses a new PIN for his token or may get access to a few emergency passcodes (lost token) or may resynchronize the clock on his token with the authentication server.
Password synchronization	The Windows login screen or Ctrl-Alt-Del screen.	Current Active Directory password	The user chooses a new password for AD. The synchronization process picks it up from a domain controller, subjects the proposed password to an extra security policy and if the password is acceptable, pushes the new password out to other systems, in addition to Windows.

Scenario	Accessed from	User authenticates with	Administrative actions
Key recovery for full disk encryption	Disk encryption software presents a key recovery mode prior to the operating system starting. The user interacts both with this screen and with a telephone based self-service system.	Answering security questions, voice biometric, etc.	The user first authenticates to the phone system, then acts as an intermediary between the challenge/response agents on his PC and on the key recovery server. After passing two or more strings of digits between the two systems, the user can choose a new password for activating his hard disk.
Integrated enrollment	Users invited to act via e-mail or web popup when they signinto their PC. Users click on a URL and complete enrollment with a web form.	His current password (e.g., Active Directory or LDAP) or his OTP or smart card pass-code.	The user answers security questions or attaches additional login IDs to his profile or dials a phone number that is displayed, keys in an authentication code and provides a voice biometric sample.

User support scenarios

Given these principles, we can envision several scenarios that improve the user experience, strengthen security and lower IT support cost:

With each of these scenarios, we leverage a shared infrastructure to authenticate users, enable users to access self-service from on-premises or remotely, from the workstation login screen, a telephone or a web browser and enable users to resolve whatever login problem they may be having without resorting to a call to the help desk.

This approach is illustrated in Figure 3

Summary

The user service advantage of this approach is clear: users enroll with a single system, complete a single security profile and can manage all of their authentication factors from one place.

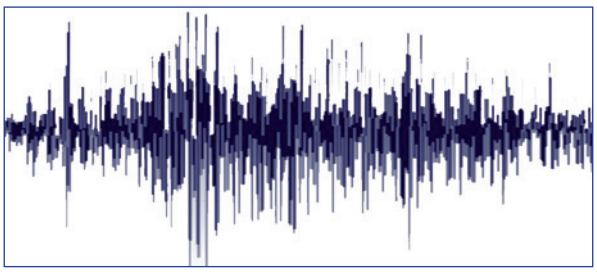
The IT cost savings advantage of this approach are also significant: login problems that currently trigger IT support incidents – for password resets, PIN resets, key recovery and more – can all be moved to a self-service infrastructure. This reduces the call volume at the help desk, especially at peak hours such as the first morning after a long weekend or holiday. Lower call volume translates to cost savings by reassigning people out of the help desk, to higher value work.

Figure 3: **Integrated authentication management:one platform for all factors**

For further information please visit www.hitachi-id.com

Voice Biometrics: Is a 'spoken token' the future of fighting fraud in the financial services industry?

By Nick Odgen, CEO and founder, Voice Commerce Group



" As the authentication procedure happens over the phone, voice biometric technology can deliver identity authorisations virtually anywhere. "

Financial fraud is a perpetual problem for the banking sector. As the industry opens up more channels to the customer, such as the internet and mobile, so it increases the opportunity for fraudsters to exploit weaknesses in their security. What's more, it seems that the industry is frequently one step behind the fraudsters; as soon as a solution is developed to combat one type of fraud, criminals are already targeting the next weakest link with sophisticated scams and approaches. As a result, payment fraud remains a significant problem for financial institutions. In its latest figures for the period January to June 2009, Financial Fraud Action UK reported a 23 per cent increase in the amount lost through card ID fraud (£23.9 million) and a staggering 55 per cent rise in online banking fraud, which suffered losses of £39 million in the six-month period. As well as hitting banks' balance sheets, fraud incidents are affecting customers' perception of their bank. However, one technology that is increasingly being discussed to help combat the problem is voice authentication. Not only does it prevent fraud, but it can also save financial institutions money and make identification and verification more convenient for the customer. This article will delve deeper into the fraud challenges currently facing the banking industry, look at the solutions made available to date to combat the problem and discuss how voice authentication can help solve some of the issues that still beset the industry.

The scale of the problem

The indomitable rise in electronic payments has played a significant role in the growing payment fraud problem. The volume of card payments has increased exponentially in recent years, as has customer usage of the internet for both banking and shopping. Emerging payment technologies, such as contactless and mobile, are further supporting the demise of cash. This range of electronic payment channels provides rich pickings for technology savvy fraudsters who are constantly evolving new and increasingly sophisticated scams for targeting these transactions. As a result, the fraud landscape is a fast moving, hard to quantify and ever-evolving issue.

Within this payment fraud landscape, identity fraud is one of the fastest growing crimes in Europe[1] and comes in many forms, such as 'skimming', 'phishing' and the use of stolen cards to make fraudulent transactions. A recent case in the United States highlighted the risks to small businesses of using online banking. Criminals stole more than $450,000 from a Pennsylvania Housing Development Authority after infecting its computer systems with the notorious Clampi Trojan. In Europe, Zeus is the latest Trojan to make the headlines by stealing banking information through keystroke logging and has led to the theft of more than £6m from online bank accounts. The Trojan is also targeting social networking sites such as Facebook and Twitter to quickly spread the viruses and malicious codes. Greater online banking security involving further identification stages than simply inputting log in details and passwords would have helped prevent the likelihood of these kinds of attack.

Fighting back

Of course, industry wide measures and standards are in place to help combat the fraud problem and innovative solutions are regularly introduced to the market. Incidents of card fraud

in face-to-face and point-of-sale environments have dropped considerably, for example, following the migration to EMV and the increased use of Chip and PIN as a form of two-factor authentication across many parts of the world. With the SEPA Cards Framework in Europe mandating the EMV standard, as well as other significant migrations in countries such as Canada and Australia, we can expect cardholder present fraud to continue its decline worldwide. EMV has not, however, fully addressed the omnipresent threat of online banking or e-commerce fraud.

Some banks, such as Barclays in the UK, have issued EMV card readers to online banking customers which provide a second layer of authentication when conducting transactions online. The card schemes have also introduced their own solutions - MasterCard SecureCode and Verified by Visa - which also provide a form of two-factor authentication for online purchases. Yet, uptake of these initiatives has been patchy at best with consumers often articulating the inconvenience of these security measures which either require them to carry around additional pieces of hardware (i.e. CAP readers), or to remember additional passwords.

Despite the measures implemented to confirm a person is who they say they are, many banks still see an identification and verification failure rate of between five to 10 per cent with their existing systems. PINs and passwords are themselves easily compromised through intentional theft, user apathy or shoulder surfing – when fraudsters look over their target's shoulder when for example withdrawing money from an ATM to steal their personal information.

The rise of voice biometrics

In addition to the solutions already discussed, biometric technology is increasingly gaining prominence and credibility in the fight against fraud. It is, arguably, one of the most advanced methods of identity verification and is slowly but surely becoming a technology that more and more financial institutions are considering as part of their anti-fraud strategy.

Rather than increasing complexity and relying on two parties taking numerous measures to authorise transactions, the beauty of voice biometrics is in its simplicity. The technology verifies an individual through their unique 'voice signature' in a similar way to fingerprint matching, iris recognition and blood DNA.

With e-commerce and online banking volumes sky-rocketing and 95 per cent of the UK population having a mobile phone, voice signatures simply slot together two favoured mediums of technology – mobile and internet - to change fraud prevention from an annoying and time consuming obstacle, to a simple and natural part of the transaction process.

As the authentication procedure happens over the phone, voice biometric technology can deliver identity authorisations virtually anywhere. The system calls your mobile and can guarantee transactional security when making a payment, protecting users against personal data compromise. As the technology works by verifying who is talking, rather than what is being said, suspected imposters or potential fraudsters are picked up and transactions re-qualified. This not only improves customer service but reduces the risk of fraud and identity theft. Furthermore, the risk of phishing is negated as card details no longer need to be divulged when making a purchase.

Biometric technology is probably the singular most powerful solution to combating fraud available today. We've seen significant investment in voice authentication in recent years, with countries such as Canada, Australia and the United States being particularly advanced in their adoption of this technology. It is also becoming increasingly used by financial institutions in the UK.

A spoken token

Peoples' voices are unique, just like their finger prints. Voice authentication analyses voice samples to extract key characteristics of a person's voice based on, for example, their vocal tract length and shape, nasal cavity size and shape, their pitch, speaking rate and prosody.

This set of characteristics taken together is called a voice print – an individual's 'spoken token'. When a genuine customer enrols with a system, a voice sample is collected and a voice print is extracted and stored for future use. When the caller speaks to the organisation again, a second voice sample is collected and compared to the previously stored voice print. This comparison generates a confidence score as to whether the voice matches the existing voice print – the caller is either accepted, and gains access to the system, or is rejected as a poor match.

Voice authentication has developed considerably in recent years and is now state of the art, with a high accuracy rate. Not only can it filter out background noise, but it is capable of recognising and accepting changes in a person's voice, as a result of a cold or ageing, for example. As a voice print is almost impossible to impersonate, it is infinitely more secure than a credit card or PIN. In fact, a voice print is the second most unique characteristic after the iris and is the only biometric that can be verified remotely, making it the most convenient biometric to use. Of course, like all security processes, voice authentication is best used in conjunction with a second factor, such as, something a user has (e.g. a credit card, ID card or mobile phone) and/or something a user knows (e.g. postal code, date of birth).

However typically, automated voice authentication is quicker than traditional methods, thereby saving banks time and money. In fact, according to a report by the centre for economic and business research, automated voice authentication could save UK financial services companies £472 million per year. Those organisations that have

implemented the technology for security purposes have also benefited from being able to provide an improved customer service experience. Automated voice authentication is less invasive for the customer as it removes the need for lengthy and unpopular interrogation by call centre agents, for example.

Improving customer service

Many banks are realising that a more precise and automated identification and verification process will allow them to begin to offer more and new automated services, which up to this point, have only been available through agents. These include personalised menus when customers call (such as 'Your account balance is £650.00, and your last deposit was recorded yesterday, can I help you with anything else?'). Automation of riskier transactions, that are dependent on stronger security, such as change of address and reporting lost cards, is also possible. Combining these applications lead to a better and more secure user experience and, consequently, happier customers.

Customer satisfaction will have a growing importance in banks' long-term strategies as competition in the sector intensifies and financial institutions are subject to more stringent regulation, much of which is aimed at providing further protection for the customer. A good example of this more stringent oversight is the new ruling from the UK's Financial Services Authority that banks must refund customers first, before investigating how a disputed or fraudulent transaction occurred. This initiative follows complaints from customers who have had problems claiming money back from their banks when they believe their card has been fraudulently used with the correct PIN. Such a clear call to action for banks surely won't go unnoticed as paying first and investigating later could lead to even greater pay-outs. From the point of view of a financial institution, preventing fraudulent transactions in the first place is now more important than ever before and the simple and effective process offered by voice biometrics should have an important role to play in supporting banks in the fight against fraud.

The key with any security offered however is to find the right balance between the level of security offered and the convenience for the customer. While customers are undoubtedly concerned about fraud, they will shy away from systems that are cumbersome or time consuming to use, leaving themselves and the bank exposed. Not only is voice authentication user friendly, it offers a highly effective, affordable and convenient solution to a financial institution's security issues, making it a candidate for widespread adoption. Its prevalence could pre-empt the end of passwords and PINs, giving rise to a ubiquitous 'spoken token'.

[1] The National Identity Fraud Prevention 2008 survey http://www.finextra.com/fullpr.asp?id=30891

For further information contact: www.voicecommerce group.com

The European Digital Agenda

By the General Secretariat of EUROSMART

Source: **Europa**

In 2009, the Smart Security Industry showed a strong resilience to the economic crisis, and Eurosmart confirmed the expectation of growth in Smart Secure Devices shipments in 2010. This industry demonstrates that its role in making citizens' digital life more secure and more convenient is more than ever on the critical path for strategic markets such as Telecom, Payment, eGovernment, Enterprise IT and Transport. The European Commission has precisely integrated this challenge in the framework of the European Strategy entitled "Europe 2020".

The European Union is indeed playing a decisive role in making the digital single market a reality. The new strategy for the Information Society, the "Digital Agenda", was adopted in May 2010. It identifies several obstacles preventing ICT to develop and deliver better services, such as: fragmented digital markets, lack of interoperability, rising cybercrime and risk of low trust in networks, lack of investment in networks, insufficient research and innovation efforts, lack of digital literacy and skills, missed opportunities in addressing societal challenges. Therefore, the strategy outlines seven priority areas:

- creating a digital Single Market,
- fostering greater interoperability,
- boosting internet trust and security,
- promoting much faster Internet access,
- fostering investment in research and development,
- enhancing digital literacy skills and inclusion,
- applying information and communications technologies to address challenges facing society like climate change and the ageing population.

The European Commission foresees for the next five years 100 follow-up actions in these seven areas, of which 31 should be legislative. Among its objectives, the European Commission wants to "make online and cross-border transactions straightforward". After consulting stakeholders on the implementation of the eCommerce directive and the reasons for the low rate of cross-border online shopping in Europe, the European Commission will make some legislative proposals by the beginning of 2011, for a possible review of this directive. Other measures will include a proposal of a revision of the eSignature Directive in 2011 with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems. Besides, since more secure solutions are increasingly needed, the European Commission encourages industry "to ensure interoperability based on standards and open development platforms".

Related to these challenges, it is of primary importance that the Single European Payments Area (SEPA) is completed. Therefore, the European Commission will ensure the completion of the SEPA, eventually by binding legal measures fixing an end date for migration before 2010. The emergence of an interoperable European eInvoicing framework will be facilitated through a Communication on eInvoicing and by establishing a multi-stakeholder forum.

Finally, now supervised by Viviane Reding, Commissioner for Justice, Fundamental Rights and Citizenship, the review of the legal framework for data protection is planned by the end of 2010. Dating from 1995, the EU Data Protection Directive needs to be adapted to new technological developments and needs to be taken into consideration in many EU actions. The European Data Protection Supervisor and the Article 29 Working Party, two entities of the European institutions, are in charge of elaborating recommendations in this matter.

The European Commission will remain vigilant about possible new obstacles and this Digital Agenda should evolve in the light of experience and rapid changes in technology and society. Eurosmart will carefully follow and accompany these new developments taking place at EU level.

As ICTs play a growing role in all economic sectors and in our daily life, Eurosmart Members believe that trust and security are key issues, as well as a strong need to ensure privacy and data protection in digital life, especially in the "Internet of Things" (objects talking to each other). In this context, Eurosmart is extending its scope of activities to biometrics and to the Internet of Things, in order to reflect the evolution of the Smart Security Industry and the market structure.

This article was provided by the General Secretariat of Eurosmart. For more information please visit www.eurosmart.com

European Education Connectivity Solution

Bringing Standards and Interoperability to Campus Cards in Europe

By Eugene McKenna
Chief Executive, Campus Services,
Waterford Institute of Technology

Introduction

The origin of the European Education Connectivity Solution Project (EECS) came about from the establishment of the European Campus Card Association (ECCA) in 2002. The key aim of ECCA was to introduce standards and interoperability into campus cards.

The European Campus Card Market was entering a critical growth phase at that time so it was fundamental that the issues of standards and interoperability were addressed. Subsequent to this, the EU introduced the Bologna Agreement, which listed student mobility as a key objective. The Lisbon Agenda identifies research and innovation as key enablers for the development of a European Knowledge Economy. The European Union is also investing heavily in the creation of a European Research Area (ERA) capable of delivering the types of innovation that will ensure that Europe achieves sustained world economic leadership. The mobility of academic staff and students is a key requirement for the realisation of the ERA and the mobility of students is specifically referred to in the objectives of the Bologna Declaration. However, major barriers currently inhibit mobility within Europe: the lack of information-sharing systems in areas such as Higher Education institutions being one.

ECCA examined numerous options to develop a suitable system for Higher Education institutions. It was difficult to get card technology companies to justify a business case for the research and development involved. After much research by the ECCA's standards committee a decision was taken to seek funding from the EU to assist with the development of a prototype project. An application for funding under the FP7-SME-2008-1-call was submitted. After proceeding through the review and negotiation process, the project received approval for grant aided funding.

A solid group of consortium partners was therefore formed between SMEs and RTDS. The SME partners provide a varied skill set in the services and security aspect of a campus card and the RTDs provide a blend of academic researchers who have proven experience in research and development with particular expertise in card technology.

EECS Consortium

Name	Involvement	Country
OneCard Solutions	SME	Ireland
University of Zagreb	RTD	Croatia
OPTeam	SME	Poland
Mecenat	SME	Sweden
Technical University of Lodz	RTD	Poland
Waterford Institute of Technology	RTD	Ireland

The EECS project will offer a solution to enable academic mobility within Europe by researching and developing a secure, standardised campus card system. The creation of a standard campus card system will facilitate academic mobility by allowing Higher Education institutions to share information using a common campus card that will act as a student's "electronic key" and will enable access to a student's records on secure databases. A standardised campus card will enable more efficient electronic exchange of data amongst H.E. institutions using the latest technology. In Europe many Higher Education institutions also operate campus card systems in order to facilitate access to services for students, academics and visitors i.e. point of sale, library access, access to classrooms/residences, printing and photocopying, transportation, etc. However, these systems operate in isolation on a standalone basis, providing no interoperability with other H.E. institutions card systems and this is due to the lack of system standards.

Background to campus cards

The traditional campus card in HE institutions in the past consisted of a simple PVC card with a bar code and in some cases a magnetic stripe. The main function of this card was primarily to act as a physical ID and facilitate book borrowing from the library. Whilst Europe is continuing to make advances in the development of campus card systems, particularly in the last decade, the United States is without doubt to the forefront in campus card systems. In the US these systems now play an important role in student life on campus, by providing a secure key to access a range of services and facilitating cashless payments. Very successful onecard programmes have been developed in the US since the early 1980's. Systems evolved from dining, library services, housing and security.

With these systems the campus card operates with a database that integrates with other systems. The card technology can consist of one or a combination of magnetic stripe, bar code and chip (contact or contactless). The student normally has only one card which acts as a secure key for all services both on and off the campus. Fig.1 illustrates a range of typical client applications connected to a campus card system:

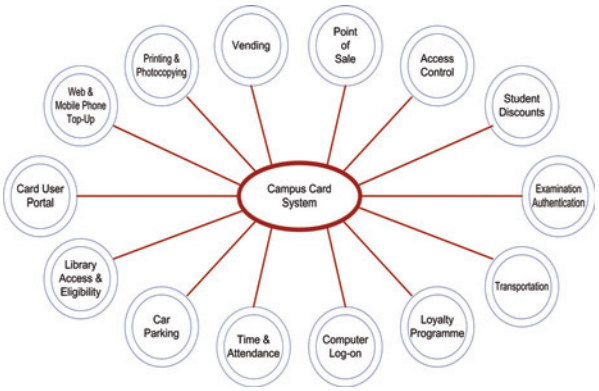


Fig. 1

The limitations of current systems

As campus card systems worldwide continue to expand, the limitations of these systems are now becoming apparent. Lack of standards, no interoperability and proprietary systems are now proving to be major drawbacks in the expansion of the campus card market. These issues are a cause of concern to campus administrators as they strive for more efficiency and cost reduction. The bespoke nature of existing campus card systems makes it extremely difficult for any company specialising in card system development and integration to justify a business case to enter the market. Therefore, as a result of these problems, the number of companies entering this market within Europe remains small. In the US and Canada the market is dominated by four/five major campus card corporations that specialise in the research, development and integration of complete systems for HE institutions.

Standards and interoperability

It is clearly evident that there is an increasing demand for interoperability in campus card systems in the European Higher Education sector. The lack of standards and design of the existing systems has created a "desert island style approach", with no interoperability or connectivity between them. Each campus system is different and built to fulfil the specific needs of the campus without any regard to the basic standard requirements of a student in terms of interoperability and mobility (e.g. the unique student number). In the vast majority of cases, each institution has its own unique numbering system with numeric or alphanumeric codes to meet its requirements, but this numbering system will have no significance in another institution in its own country, or elsewhere in Europe. With the increasing need for student mobility across Europe, it is necessary to have a system that will allow the individual university to retain its own student numbering system whilst converting the number to a common European standard for inter-communication purposes. This would be an important first step in the process of overcoming the major barrier to interoperability and connectivity in systems. The present and desired future state of the art in campus card systems is illustrated in Fig. 2

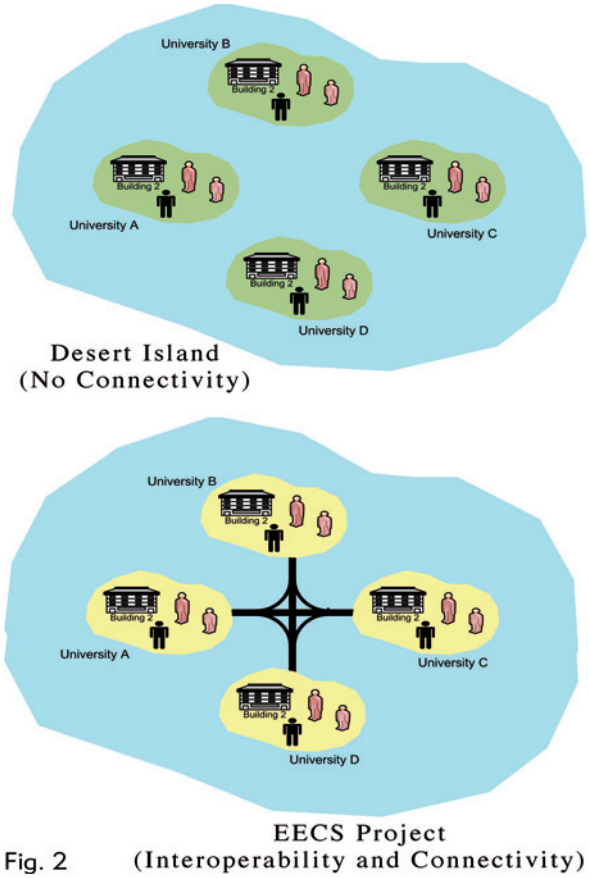


Fig. 2

The EECS consortium SME's have individually produced successful campus solutions throughout Europe. However systems are generally designed and built for the specific needs of each individual campus. This individualistic and "once-off" nature of their bespoke technology is inhibiting further progress for the market.

EECS PROJECT AIMS AND OBJECTIVES

The project was established to research and develop a solution that would overcome the barriers that currently exist in relation to the standards and interoperability between campus card systems and academic mobility across Europe.

The key aims of the project are:

(i) Undertake detailed research on the current and future state of the art in campus card systems in Europe.

(ii) Research and develop standards to achieve interoperability and facilitate the secure authentication of information transfer between educational institutions.

(iii) Build a working prototype to the recommended standards in order to facilitate interoperability.

(iv) Demonstrate the prototype in a live working environment between campus card management systems in two European countries.

The EECS consortium, consisting of three European SMEs and three academic researchers together with the European Campus Card Association (ECCA), identified the core technological and non technological requirements necessary to research and develop a prototype card system. This system will provide interoperability and connectivity between HE institutions across Europe. It will contribute to overcoming the current obstacles to exploitation of the campus card market by SMEs and will also support academic mobility by facilitating the secure transfer of student information between Higher Education Institutions. In order to achieve the overall aims of the project, the consortium identified the following four principal objectives:

Objective 1. Research the current and potential European campus card market together with the current state of the art and future requirements. This objective, which was successfully completed, involved research across 100 European HE institutions to establish the current technological state of the art and international standards. Specialised needs, legal and regulatory issues were also investigated.

Objective 2. Apply the market research results to research and design the modules for an EECS campus card prototype. This objective was successfully completed and resulted in the development of the requirements and specifications for the three core modules:

- The Card Application Management System (CAMS)
- The Client Application Interface (CAI)
- The Student Connectivity Module (SCM)

Objective 3. Build and test a full working EECS prototype. This objective, involved building, testing and validating a real working prototype, which incorporates each of the core modules. A feature of this objective will involve student exchange between two Higher Education institutions and the transfer of the required student academic information. This information transfer will be authenticated by the use of the student's campus card.

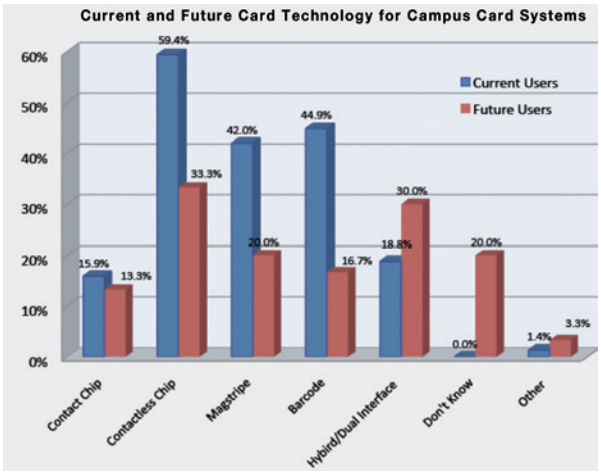
Objective 4. Develop a Marketing and Dissemination plan to inform potential customers of the new prototype campus card system. This objective is primarily concerned with informing the potential market of the EECS project.

MARKET RESEARCH

The EECS consortium carried out comprehensive research of current card management systems in the campus card industry and also researched the end user requirements directly. This process involved focus group meetings and interviews/surveys with card system integrators and staff from Higher Education institutions. It also involved meetings with the members of the European Campus Card Association. These meetings highlighted the current problems and challenges that surround the issue of interoperability and student mobility between campuses within a country and also between countries. An important part of the research undertaken was the survey which was conducted throughout Europe, involving 100 H.E. institutions. The key aim of this survey was to investigate the current and future needs of a standard European campus card for institutions that have a campus card in place and also institutions that are considering the implementation of a campus card system.

The following outlines some of the key items identified from the research. In the market survey the respondents replies are based on order of preference (where applicable).

THE CURRENT CARD TECHNOLOGY



There are five types of card technology currently in use. The above graph outlines the card technology used by institutions that have a campus card system in place (current users) along with institutions that do not have a campus card system in place (future users). 59.4% of current users use the contactless chip, and future users also outlined their preferred technology for contactless technology.

Campus Card Client Applications Trends

The table below outlines the client applications currently in use in institutions that have a card system in place and also the applications that future users would implement if or when they install a card system:

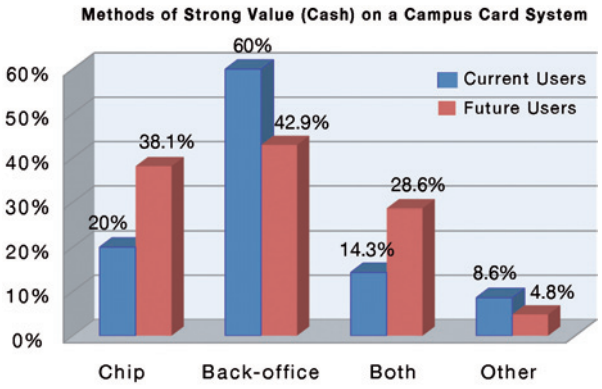
Current & Future Trends for Client Applications		
Client Applications	Current	Future
ID Card Production	71.4%	53.33%
Printing & Copying	62.9%	36.6%
Library Access	81.4%	65.5%
Library Payments	15.7%	30.0%
Car Parking	24.3%	10.0%
Time & Attendance (Student)	11.4%	36.6%
Time & Attendance (Staff)	17.1%	23.33%
Access Control	71.4%	76.7%
Vending Machines	11.4%	10.0%
Point of Sale(restaurants, shops etc)	34.3%	26.7%
Web Food Ordering	4.3%	3.33%
Computer Log-On	14.3%	33.33%
Examination Identity & Authentication	30.0%	60.7%
Student Travel Concessions	17.1%	10.0%
Public Key Infrastructure	7.1%	20.0%
Other	10.0%	13.33%

At 81.4% library access is understandably the most common client application, 71.4% have ID card production, 71.4% use their campus card for access control, 62.9% use the campus card for printing and copying, 34.3% have a point of sale application, 30% use the card for examination identity and authentication. The remaining applications include time and attendance, library payments, computer log on, vending machines, public key infrastructure and web food ordering. The most important application perceived by respondents who do not have a campus card system in place is that of access control (76.7%). Library access is also considered an important application (65.5%).

It was closely followed by examination identity and authentication (60.7%). ID card production, time and attendance (student) and computer log-on are also deemed very important applications for a campus card.

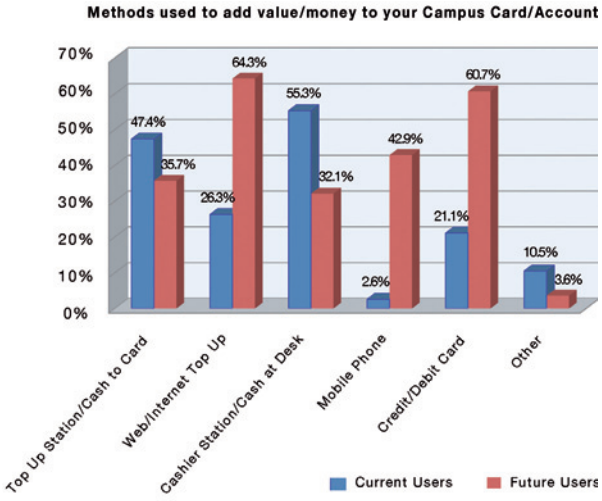
Payment Systems

The survey examined the type of methods used by current users and the preferred method by future users to store value (cash) on a campus card system as shown in the graph below:



The current users showed a clear preference for the back-office (60%), it was also the preferred choice for future users (42.9%).

The graph below illustrates both current and future user prefer-ences on how to add value/money to their campus card /account.



Of the current users, 55.3% use the cashier station/cash at desk to add value to their campus cards with 64.3% of future users preferring to top up through the web.

" The EECS project will offer a solution to enable academic mobility within Europe by researching and developing a secure, standardised campus card system. "

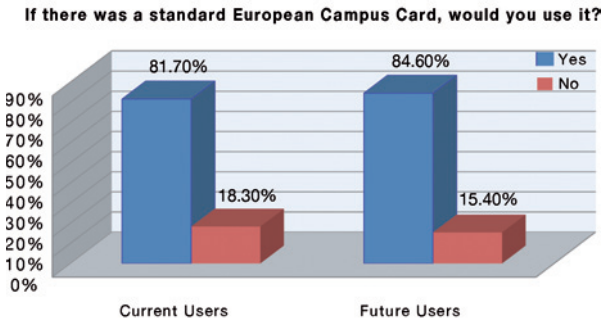
Interoperability of Campus Card Systems

To determine the importance of interoperability for campus cards, respondents were asked to rate how important they felt interoperability in a campus card system was to their institution.

The Importance of Interoperability for Campus Cards		
Importance	Current	Future
Not Important	11.1%	7.7%
Somewhat Important	34.9%	23.1%
Important	41.3%	26.9%
Very Important	12.7%	42.3%

Of the current users, 12.7% felt interoperability was very important with 41.3% stating interoperability was important. Overall 54% of this group feels that interoperability is important. 42.3% of future users rated interoperability as very important and 26.9% rated interoperability as important, showing that almost 70% rated interoperability as important. It's evident from the results that a high percentage will want to use their card in other institutions to access facilities/services. Therefore, the development of standards is of critical importance in the EECS project to achieve interoperability and mobility. It will also be a requirement to have the ability to integrate with other MIS systems and third party providers.

It was important to determine if HE Institutions, both current and future users, would use a standard European campus card system if one was available. The graph below outlines 81.7% of current users would use a standard European card and 84.6% of future users would also use one.



The market potential for the SME's is high as a considerable percentage of HE Institutions will purchase from a third party supplier as opposed to designing their own system. Therefore, the SME's need to exploit this market potential once a standard card is developed.

From the research undertaken it is evident that HE institutions require a standard European campus card which is multi-functional. The research also clearly confirmed the validity of the EECS project's vision i.e. to research and develops a solution that would overcome the barriers that currently exist in relation to the issues of standards and interoperability and also academic mobility within Europe.

EECS PROTOTYPE DEVELOPMENT

The EECS Prototype technology development involves the building of three core modules;

(i) The Card Application Management System (CAMS)
(ii) The Client Application Interface (CAI)
(iii) The Student Connectivity Module (SCM)

Fig. 3 describes in graphical form an outline of the EECS project. The example given can represent two campuses; e.g. Campus 'A' located in Ireland and Campus 'B' located in Poland. The functionality of the prototype system being developed within the EECS is built up of the three core modules, CAMS, CAI, and SCM.

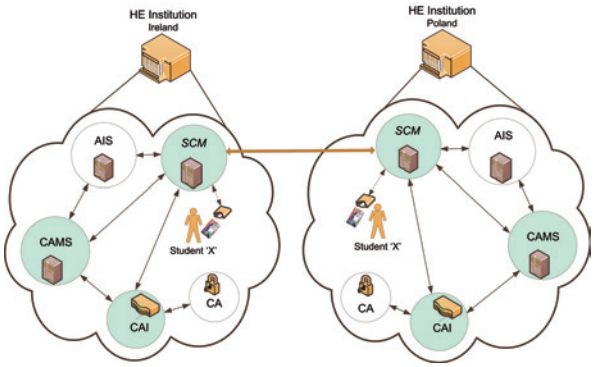


Fig. 3

THE CARD APPLICATION MANAGEMENT SYSTEM (CAMS)

The core element of a campus card system is the card application management system (CAMS). It consists of two main parts, the central database and the CAMS management software. The management software allows for Graphical User Interface (GUI)-based configuration of the main database, for example adding users, devices etc. The central database provides a backend that integrates and communicates directly with already existing Academic Information Systems (AIS) and Card Production Systems in order to produce a campus identity card (or any token). The card or token can then be used in conjunction with the CAI and SCM to authenticate and identify the user and permit access to services/facilities as required.

The CAMS and CAI will knit together to deliver a robust transactional micropayment system for vending, point of sale and other applications that require electronic payments either within or outside the campus environment. The system will also provide quick and easy access to top-up facilities and the viewing of balances via mobile technologies and web based systems.

THE CLIENT APPLICATION INTERFACE (CAI)

The Client Application Interface Module is a middle-layer component of the EECS system with the primary purpose of bridging the gap between a large number of small client applications that present a real-world interface towards con-

sumers of various services, and back-end systems controlling the system functionality and service provision.

The CAI provides key functionality for both Client Applications (CA) and the Student Connectivity Module (SCM) by connecting them to the central system. Due to the wide variety of client applications, means of communication, functions and system organisations, the CAI is essential to simplify the requirements for CAMS and integrate with it to form a fully functional system. The CAI achieves this by providing standard communication specification for current and future CA's which makes the operation of the CAMS more efficient and future proofed. The main principle is that all communication is event-based and follows exchange of standardised, device-independent request/reply messages. Data is exchanged using well known industry standards thus allowing the majority of CA's to be easily modified to integrate with the system. The communication between the CAI and CAMS database is then performed via database procedures and functions which retrieve and return data as necessary.

The Student Connectivity Module (SCM)

The Student Connectivity Module (SCM) supports student mobility; it is responsible for managing the international exchange and transfer of students' academic information. It sends and receives student mobility data to and from other Higher Education Institutions. The module communicates with the AIS and/or other databases containing information necessary for student exchange. The SCM comprises in part of an applet, which will be used to communicate via the CAI with the CAMS database. An Authentication Token, normally a campus card, will be presented to the applet in order to authenticate a user (student). This will trigger the begin-ning of an 'event' i.e. an instruction to authenticate the user will be sent to the CAI, which will call the corresponding procedure within the CAMS database. Once authenticated, the SCM module then receives data from the HE Institution database, and not from the authentication token.

EECS Consortium

Partner 1 – OneCard Solutions, OCS, Ireland

OneCard Solutions was established in 2002 to provide a wide range of highly reliable solutions that have advanced the development of card technology. OCS offers a wide range of services including identification, point of sale, access control, printing/photocopying, library access, and vending, as well as offering web-based and mobile phone top-up options in conjunction with the users debit or credit card. OCS is a corporate member of the European Campus Card Association.

Partner 2 – University of Zagreb, Faculty of Electrical Engineering and Computing, Croatia

University of Zagreb, Croatia, was established in 1669 and is the oldest and largest university in South-Eastern Europe. University of Zagreb consists of 29 faculties, three art academies and the Centre for Croatian Studies. It is the largest teaching institution in Croatia with its comprehensive programmes and over 50,000 full-time undergraduate and postgraduate students. University of Zagreb is a research-oriented institution, contributing over 50 percent to the total research output of Croatia.

Partner 3 – OPTeam SA, Poland

OPTeam was established in 1988 as a system integrator and software developer. Today OPTeam specialises in smart card based systems and network security. The company developed its own systems for retail, financial and university education sectors. OPTeam delivers software systems and infrastructure for loyalty card and corporate card systems as well as software applications for payment card acceptation.
OPTeam is a corporate member of the European Campus Card Association.

Partner 4 – Mecenat, Sweden

Mecenat was founded in 1985 and has since worked with discounts for youths. In 1998 Mecenat received a request from The National Swedish Board of Student Aid (CSN) to produce their student identification card (CSN-card) and Mecenat have done this ever since. Mecenat verify students for companies and organisations. They produce and distribute more than one million student identification cards each year. These cards are valid for student discounts on thousands of products and services. Mecenat is a corporate member of the European Campus Card Association.

Partner 5 – Technical University of Lodz, TUL, Poland

Technical University of Lodz (TUL, Politechnika Lodzka), established in 1945, is located in the central part of Poland. Currently TUL employs about 3,000 staff members (incl. about 1500 academics) and has more than 20,000 students enrolled in BSc and MSc courses. There are over 500 students enrolled at TUL on PhD studies. TUL faculty members have participated in numerous national and international research projects including 45 projects realised within the European framework programmes (FP5, FP6, and FP7).

Partner 6 – Card Technology Research Centre, Ireland

The Card Technology Research Centre (CTRC) at Waterford Institute of Technology is the leading research centre in card technology in Ireland. The CTRC was established to create a centre of excellence in research, innovation, design and training in a wide field that includes: card technology, campus solutions, standardisation and interoperability of card systems. The CTRC has been involved in numerous projects throughout Europe and the USA.

For further information please contact EECS Project Administrator at: eecs@onecard.ie or visit the EECS Project website: www.eecscard.eu or the European Campus Card Association website: www.ecca.eu. To contact the author please email emckenna@wit.ie

Digital Tachograph –
a smart way to more security on Europe's roads

By Klaus-Peter Schmidt, Program Manager, Identification, Morpho, e-Documents Division

Security is a term closely linked with smart cards. Yet they can also ensure more safety in everyday life, a fact visibly demonstrated by rollout of the digital tachograph: here, technology helps improve the options for controlling the times at which truck and bus drivers are behind the wheel or are resting, and thus avoid accidents and ultimately save lives.

European Union creates statutory foundation

Siim Kallas, vice-president of the European Commission in charge of transport, recently stated that the EU intends to halve the number of road deaths in Europe by 2020. The number of deaths caused by road accidents has already been cut by more than 40 percent since 2001, but the EU aims to improve safety on Europe's roads even further. One of the measures introduced as part of this major political objective is the standardization of the working conditions for drivers of commercial trucks and busses; in addition, regulations that govern the working time of crews of vehicles engaged in road transport will be added, or existing ones revised.

The decision was made to replace the analog tachograph and its familiar paper disk with an electronic solution in order to ensure better control of the times at which truck and bus drivers are behind the wheel or are resting. Since May 2006, all newly registered vehicles in the EU with a total weight in excess of 3.5 tons, and buses with more than nine seats, must be equipped with the digital tachograph.

COUNCIL REGULATION (EEC) No 3821/85 of December 20, 1985 prescribes the control of driving times and rest periods through the use of recording equipment in road transport that must always be adapted to technical progress. Since June 2002, smart cards have been a firm part of the technical specifications for the digital tachograph.

How does the digital tachograph work?

The overall system comprises four different types of card, the vehicle unit (VU) and the motion sensor.

The motion sensor reports information on the distance covered to the vehicle unit, where this data is captured, processed and stored. However, at this stage the recorded information is not clearly assigned to a specific driver. This task is undertaken using a driver card that can be inserted in the vehicle unit and enables the driving times and rest periods to be stored electronically for the specific driver in the vehicle unit and on the card. Given average driving activity, the data for the driver remains in the vehicle unit for at least 365 days and on the card for at least 28 days. This data can be accessed by either the transport company or supervisory authorities – via a company card for the transport company and a control card for the supervisory authority. Reading the data on the driver card requires that both it and the control or company card must be inserted in the vehicle unit, which has slots for two cards to permit this. The data can be downloaded via an interface and stored on a special medium (download key, stick) or output to a printer integrated in the vehicle unit.

In addition to the driver's activities all these other activities are recorded in the vehicle unit as well and are available for further analysis. The fourth type of card – the workshop card – is required during installation of vehicle unit and motion sensor and whenever repairs on these components are carried out. In addition, the workshop card can be used to make a wide range of settings on the vehicle's control unit. Due to its special very sensitive role, this card comes with a PIN that must be entered on the vehicle unit whenever the card is used.

The driver card is tied to a specific person: it must be possible to record the driver's activities so that they can be traced. A photograph of the driver is prescribed so that he or she can be easily identified when controlled. The EU recommendation is to individualize the workshop and the control card as well, even if the regulation does not require that as mandatory. The individualization of these two cards provides better traceability of the records since the activities of Tachograph fitters and supervisory authorities are linked to a dedicated person.

The role of the smart card

One of the main weaknesses of the old analog tachograph was and still is the ease with which it can be manipulated. If the driver does not insert the paper disk, the tachograph does not record any activity. The disk can simply be destroyed and replaced with a new one after driver has violated the prescribed driving times and rest periods.

With the new digital tachograph, drivers might also hit on the idea of simply not inserting their cards. However, in contrast to the old paper-based solution, the vehicle's activity is still recorded in the vehicle unit, so that this type of fraud can now be discovered and the transport company can be called to account for the violation.

Since all data are now available in electronic form, a lot of services and applications are available to support the

transport company to fulfill their juridical obligations. E.g. the archiving of the driver's activities can be outsourced to external services guaranteeing save and law compliant storage of data or the data can be used for faster and more detailed invoicing or fleet management.

To make daily life easier and to support the transport companies and drivers in their work, Morpho's Tachograph cards enable data to be downloaded from the driver card to external devices and helps to save time during the compulsory bureaucratic effort of archiving data.

Secure data recording

The authenticity of the data recorded by the digital tachograph must be ensured so that it has probative force. The smart card vendor Morpho, which supplies tachograph technology to twelve European countries, supports the cryptographic overall system based on a hierarchical PKI infrastructure using asymmetrical 1024-bit RSA keys, with the private/secret key stored on the device or card.

The public part of the key (public key) is signed by a national certification authority (CA) in the form of an electronic signature, and this certificate is then stored on the card or vehicle unit. When a tachograph card is inserted in the vehicle unit in actual use, the card and unit exchange these certificates and can verify that they are genuine by means of cryptographic calculations. No data is transferred until they have verified the certificates. This procedure ensures that only 'genuine' cards and units exchange data, and as a result, the data's authenticity is ensured.

The hierarchical international PKI

Under the EU Regulation, every country participating in the digital tachograph system must run a national certification authority (CA). An RSA key pair must also be generated at every CA to sign the electronic certificates of cards and vehicle units. To ensure that the card and vehicle unit can authenticate themselves when the certificates are exchanged, the certificates must be signed with the same key by the same national authority. A higher-level instance is required to guarantee that a card that has been created in Country 1 and has certificates from that country's certification authority can exchange data securely with a vehicle unit from Country 2. This higher level instance is an organization that holds the root certificate, which is likewise based on 1024-bit RSA keys. The public key of every national certification authority is stored in a member state certificate and signed by the highest certification instance (root certification authority). The card and vehicle unit use cryptographic calculation methods to establish whether the certificates issued by the various national authorities have been signed by the same higher-level instance and are therefore trustworthy. This international hierarchical cryptographic infrastructure ensures that the stored data's origin can be defined unambiguously and that it can be used as legally valid evidence.

Security policy for a pan-European system

The root CA is run by the EU and is located at the Joint Research Centre (JRC) in Ispra, Italy. The JRC is an EU research institute and supports European policy with technical and scientific services. The JRC has defined the security requirements for the overall system in a general European Tachograph Security Policy. This is implemented by the participating states in the form of national security policies, which naturally must comply at the very least with the requirements of the European Security Policy. The national security policy details the security requirements for the various instances required for producing and issuing the tachograph cards at the national level. For instance, it stipulates the precise requirements for creating the RSA key pair so that this security-critical process is handled with the requisite sensitivity. The national security policy is assessed by the JRC and, if necessary, revised in cooperation with the national authorities. In national implementation of the security requirements, every instance involved must furnish proof – in what is called a practice statement – that the requirements have been put into effect. This practice statement is often assessed by independent experts and the results of this are made available to the national authorities. The process may sound somewhat formal, but it ensures security in the production and personalization of the cards.

Of course, it is also necessary to ensure that the data, certificates and keys on the cards and in the vehicle units are protected against subsequent manipulation. The technical specifications govern in detail how the data, certificates and keys are stored and how the data can be accessed. Some data, such as the 'EF_Identification', which contains the name of the driver, among other things, can always be read ('read always'), but never overwritten ('update never'). Other data, for example the 'EF_Events_Data', which stores activities along with a universal time code stamp, can always be read, but only updated after successful authentication with the vehicle unit ('update AUT').

Naturally, the private key cannot be read by any instance. Just about all the data on the card is stored in unencrypted form; the 'EF_Sensor_Installation_Data' is stored in encrypted form on the workshop card.

Nothing is possible without a security certificate

The security certificate offers proof that the security requirements for accessing the data are complied with. The manufacturer of the tachograph cards or vehicle units must hold this certificate. In Germany, for example, the certificate is issued by the German Federal Office for Information Security (BSI). In a complex process, the vendor of the operating system must prove that it fulfills the security requirements. These requirements are defined by what are called protection profiles, which are available in different levels. The tachograph cards must meet the requirements of the Common Criteria EAL4+ or ITSEC E3 high protection

High Security Printing Conferences

RECONNAISSANCE *international*
PUBLISHERS AND CONSULTANTS

Cross Conferences hold two regional conferences each year
for the High Security Printing, e-Passport, ID and related industries

From the Industry - For the Industry

8th PAN EUROPEAN HIGH SECURITY PRINTING CONFERENCE and TWO HALF DAY WORKSHOPS

8 - 10 MARCH 2011

Austria Trend Hotel Savoyen - Vienna, Austria

Sponsors - Security Printing Alliance (Jura, Parvis, OeBS), Gemalto, OeSD and Digital Identification Solutions

The regional high security printing conference for

Russia, Eastern/Central Europe

THE 10th ASIAN HIGH SECURITY PRINTING CONFERENCE and TWO HALF DAY WORKSHOPS

7 - 9 DECEMBER 2011

Leela Kempinski Hotel - New Delhi, India

Sponsor - Digital Identification Solutions

The regional high security printing conference for

Asia/Australasia

Each Conference features:

- 2 day High Security Printing Conference
- Two Half-Day Workshops
- Complimentary Gala Dinner
- Sponsorship Opportunities

Conferences include:

2011 – Vienna	and	New Delhi
2010 – Berlin	and	Kuala Lumpur
2009 – Warsaw	and	Beijing
2008 – Prague	and	Bangkok
2007 – Budapest	and	Hong Kong
2006 – Sofia	and	Kuala Lumpur
2005 – Kiev	and	Hanoi
2004 – Berlin	and	Jakarta
2003 – St Petersburg	and	Shanghai
2002 – Budapest	and	Bangkok
2001 – Moscow		

CROSS

SECURITY PRINTING
CONFERENCES
PART OF
RECONNAISSANCE
international

Email: info@cross-conferences.com
Website: www.cross-conferences.com
Tel: +44 (0)1932 785680
Fax: +44 (0)1932 780790

Market Leaders in Regional High Security Printing Conferences

profiles. After extensive testing has been conducted by independent experts, the test report/expert report on compliance with the protection profiles is submitted to the BSI and examined in the subsequent certification process. After this procedure has been successfully completed, the BSI issues the security certificate to the operating system vendor.

Type approval

The vehicle units are installed in the vehicles together with the motion sensor and used in everyday road traffic along with the tachograph cards. The EU Regulation therefore prescribes type approval for the components used: every producer of one of these three components must hold type approval for its products. Type approval applies EU-wide and is essentially based on three pillars:

- *Security certificate*
  The security certificate is the proof that the security requirements demanded for the operating system of the tachograph cards are fulfilled and thus that the security of the data stored on the cards is ensured.

- *Functional certificate*
  The functional certificate demonstrates that the cards meet the required physical properties. First of all, the authority responsible for type approval must be provided with an independent report confirming that the cards meet geometry requirements, have passed various mechanical stressing tests and that the electrical parameters for data communication with the vehicle unit are observed. The functional certificate is then issued by the type approving authority.

- *Interoperability certificate*
  The JRC in Ispra tests the interaction between the various components to make sure that the cards work smoothly with all vehicle units that have already been awarded type approval. Along with the security and functional certificate, the card vendor provides the JRC's test lab with several sets of test cards. The cards are not given any 'genuine' certificates from a national CA; instead, they receive test certificates that the JRC has created in a test environment with a test root CA. The cards only work in vehicle units that also contain the test certificates. After a defined testing procedure, each card type is subjected to a wide range of different use scenarios in all vehicle units to examine the components' interaction. New vehicle units also undergo this procedure and must prove that they interact with all the cards that have been awarded type approval.

This complex system for ensuring security in the production and personalization of the cards (data security, operational reliability, etc.) must be complemented by measures for card application and issuance so that the possibilities of misuse and manipulation are restricted in this process, too. When cards are applied for or issued, the driver's identity is checked in order to prevent him or her from holding more than one driver card. If the card is lost or is faulty, indices in the card number are incremented when the new replacement card is produced so that the different cards can be distinguished. This is important because citizens are allowed to choose their place of residence freely within the EU, and a driver might attempt to apply for a driver card in another member state. In cases where there is the possibility that a second card is being applied for, the card-issuing authority can inquire from other member states whether the driver has already received or applied for a card there. To enable this, the EU has launched a network named TACHOnet. Beyond this, cards that have been lost or whose holders have lost their driver's license are also blacklisted in TACHOnet, and these blacklists are available to authorities when they make road side checks.

A smart approach to achieving greater safety – even outside the EU

The digital tachograph has even spread beyond the borders of the EU. A number of non-EU states (Norway, Iceland, Liechtenstein and Switzerland) have been quick to join this system under agreements with the EU. However, the greatest expansion has been achieved through an extension to a UN (United Nations) transport agreement in 2006, in which most European states, including ones outside the EU, have undertaken to introduce the tachograph. This European Agreement concerning the Work of Crews of Vehicles engaged in International Road Transport ("Accord Européen sur les Transports Routiers" or AETR) has stipulated since June 2010 that trucks and busses registered for the first time and used for international transport must be equipped with a digital tachograph. Many participating states have not implemented the agreement by the deadline originally envisaged, in part due to the effects of the financial and economic crisis. In the meantime, however, just about all participating states are working on implementation and preparations to issue the cards within the extended schedule to end of 2010.

With every accident that can be avoided thanks to well-rested bus and truck drivers, tachograph cards make a concrete contribution to safety on Europe's roads. The system is not fully mature in all aspects, but the initial resistance to its introduction has given way to a realistic viewpoint and development of the benefits of the new electronic system. Work is underway to eliminate the existing minor weaknesses in everyday operation and further restrict the possibilities of manipulation.

For further information please email klaus-peter.schmidt@sagem-orga.com or visit www.morpho.com/e-documents

Universal Identity: Perspective from India

By Manju Murthy, Payments Consultant

Executive Summary

Broad-based government-mandated issuance of identity credentials is a controversial initiative. Nonetheless, in an emerging country, identity credentials can be a valuable enabling infrastructure to help the economy lead in the 21st century. This article will look at the India's Unique ID initiative, Aadhaar, from a business perspective and in the context of the government delivering subsidies and services.

Introduction

Universal identity credentials are turning out to be the foundation of modern digital society. Whether one wants their government to be involved with aggregating and managing such information is a controversial topic. Countries like Singapore have pulled it off successfully and are reaping the benefits of universal identity. Countries like the US, due to the fear of big brother, may not go down this path just yet.

Universal Identity - Foundation of the Digital economy

In a world plagued by electronic fraud, identity theft, funding of terrorism, money laundering..., service providers are mandated to know their customers (KYC). In a world where consumers are used to instant gratification, consumers are not interested in waiting for service providers to process KYC documentation before consumers can start using the services. Additionally, when the lifetime value of customers is low, like in India, the fixed costs associated with meeting the KYC norms destroy the feasibility of many businesses. A universally accepted [federated] identity addresses the above concerns in one shot.

While private enterprise issues identity credentials (e.g., Equifax), their use and sphere of impact is intentionally limited. It is widely believed that only the government has the ability to be the issuer of [broad-based] identity credentials, primarily due to liability concerns in case of identity fraud.

The Indian government, in a bold stroke of genius/naiveté has jumped on the universal identity bandwagon. Aadhaar, India's Universal Identity program[1], is a bold move by the government with aggressive timelines and associated funding. This initiative plans to issue 100M credentials in its first year[2] (budget of $413M @ INR46/1$), and a total of 600M credentials over 4 years (estimated cost of $1.4B). The scope of coverage is comprehensive, which includes both urban and rural India. Aadhaar credentials are to be distributed to all residents of India. Another reason for the buzz around Aadhaar is that it is lead by Mr Nandan Nilekani, co-founder of Infosys.

History

Like any other society, Indians have also been issued many credentials. PAN (by the Income Tax department), Voter's ID Card (Election Commission), Ration Card (to BPL citizens)... However, India has been impacted by fraud associated with fake identity credentials. Over 1 million duplicate PAN Cards have been in circulation, which are getting cleaned up (source)[3]. Starting with a clean slate by issuing identity credentials is a way to get around existing problems.

The initial objective of Aadhaar is to improve efficiency and efficacy of delivery of government subsidies, grants and services to its residents (primarily the poor). I will not discuss here the likelihood of Aadhaar being able to address the related ills that plague government programs. However, I will keep the focus of this article to identity credentials to poor in India, which is about 200-300 million citizens.

Authentication Factors associated with Identity: To repeat a cliché about India, India has many Indias in it. A broad-based program like Aadhaar that touches each resident needs to be built on the least common denominator across a diverse

populace. This least common denominator happens to be a unique number that is assigned to the individual. This is the what you have factor (not a card, but just the number). In a land where literacy is not universal, the what you know factor is difficult to implement. The who you are factor is biometrics. Fingerprints have formed the proof of identity in rural India and is culturally acceptable.

At the time of registration, the individual is assigned and issued a unique number (12-digit number). Subsequently, at the time of accessing any service that requires proof-of-identity, the individual provides their unique ID and swipes their fingers against the fingerprint reader. This is easy enough and can be an affordable system.

Please note that the Aadhaar does not issue a card or token as proof of identity. This practical decision by Aadhaar increases chances of its success and keeps the implementation costs low.

History of Identity Cards in Rural India: Over the past many years, government and private service providers, have been issuing identity credentials to poor. Barcodes, Magstripe cards, contactless memory cards, contactless processor cards and smart cards have been issued. The harsh environment/ambient conditions of villagers (dust, dirt...), are not favorable to carrying cards. The life of physical cards are extremely short and support costs high. Consequently, based on the card issuer and the context of the usage of identity credentials, the issuer can decide the what you have media. Biometrics: Fingerprints have been a tricky factor for authentication. About 10% of the rural poor have their finger prints smudged from years of working their fields. Retina scanners are still very expensive for mass deployments. Nonetheless, the ecosystem is rallying around this wonderful opportunity to solve these basic problems.

Innovations

Most things that China and India do result in mind-boggling numbers.

- Managing about 600M identity credentials in a low-cost manner could result in innovations in distributed architecture.
- Need for large-scale deployment of finger-print scanners is expected to drop the price of scanners to a fraction of their current costs, as well as, create a base of indigenous manufacturers.
- Another side-effect of affordable finger-print scanners might be the resulting ubiquity of this feature in mobile devices.
- As India grapples with citizens with smudged / missing finger-prints, we might see low-cost retina scanners (or similar biometric scanners) emerge.

Usage models of identity credentials

- MGNREGS: Mahatma Gandhi National Rural Employment Guarantee Scheme (MGNREGS) is a rural employment guarantee scheme that provides qualifying households work for a minimum number of days (e.g., 100 days) at a minimum wage. Identity validation is a core aspect of the implementation process, including during registration, availing benefits, funds dispersion...
- MicroATM: In rural India, bank branches are not practical and/or feasible in remote locations or sparsely populated villages. MicroATM is a low-cost device which offers frequently used branch services, thereby saving banks the cost of opening branches and the consumers the trouble of getting to a bank. These devices would accept and validate identity credentials as part of the service delivery process.
- Mobile POS: In a country where 600M mobile phones exist, mobile phone based devices are a cost-effective alternative to the single purpose EDC/POS terminals. Mobile POS devices, used by merchants/banks, have the ability to validate identity credentials before the consumer can access funds in their accounts.
- Public Distribution System (PDS): Government benefits include a set of staple set of essential commodities. Distribution of these benefits has been affected by pilferage and benefits end up in the wrong hands. Use of identity credentials are seen as a mechanism to bring about transparency and efficiency in the delivery process.

Criticism

In any project that involves issuing identity credentials [to all its residents/citizens], civil liberties and privacy concerns are among the many concerns. Additionally, biometrics and other PII data of 600M citizens is a juicy target for criminals.

Summary

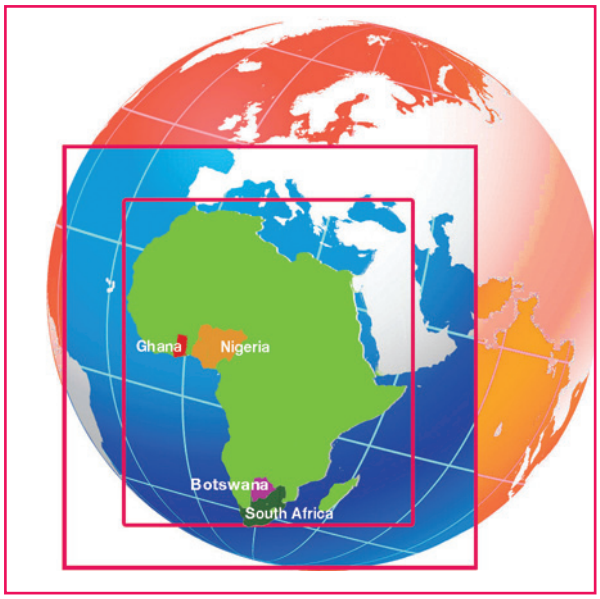
While, on paper, Aadhaar is the right thing to do, it is debatable whether Aadhaar will be a success. Additionally, given the many demands that the government has in addressing the needs of the poor, the investment in Aadhaar has been questioned. Having said that, universal identity for its citizen may well show up as a necessary infrastructure requirement for the leading nations in the 21st century.

1 http://uidai.gov.in/
2 http://www.business-standard.com/india/news/uidai-sets-target10-cr-%5Caadhaar%5C-numbers-in-one-year/100969/on
3 http://www.moneycontrol.com/news/business/pan-scam-ii_292385.html

For further information email manju.murthy@gmail.com.

Analysis of Identification Systems Adoption in Selected African Countries

By Joseph Kwame Adjei, Center for Communication, Media and Information Technologies [CMI]



Introduction

Governments all over the world are currently in the process of implementing identity management systems (IDMS) to facilitate privacy protection, commercial activity, and ensuring the rights of citizens (1)and (2). In spite of numerous studies on technology adoption, little is known about factors affecting adoption of electronic identity management systems (e-IdMS) from a developing countries perspective. Using the experiences of Ghana, Nigeria, Botswana and South Africa, we analyze electronic identity management technology adoption and their impact in selected African countries. The subsequent section deals with technological development in Africa followed by a brief analysis of technology adoption theory. We then focus on the era of biometrics and discuss specific biometric implementations in selected African countries. We conclude by discussing the specific issues and finding from the study.

Technological Development in Africa

Developing countries in Africa, like many other parts of the world, are technologically lagging behind due to several years of primitive cultural practices, bad governance, chaotic climatic conditions, poverty and illiteracy. A major problem is the lack of proper record keeping. Historically, founders have used natural disasters, landmark events and tribal body marks as means of identification and reference points. These practices, which have in the past served their purposes, have in this age of rapid technological development proved very slow and unreliable, leading to improper forms of identification and authentication and incorrect demographic statistics.

The emergence of mobile phones and the rampant growth of cellular networks have made instant and reliable communication a reality in Africa. Connectivity in Africa is essentially assisting in making individual people count. This growth has been driven by the fact that generally African countries are "technological green fields" in the sense that there are no legacy systems to contend with. With no reliable addresses, street and location codes, cell phone numbers have become the most reliable means of identification. Hence, the reluctance of businesses and government to write off undepreciated and paid-for infrastructure does not become an issue in developing countries since usually there are none.

This tremendous growth in cellular communication, in many African countries has become a major impetus for positive responses to IdM projects. For instance, only 20 % of families in Africa have bank accounts, and in Nigeria with a population of about 140 millions (3) there are only 30 million bank accounts, 30 % of which are corporate accounts. Whilst in Ghana only 5% (1.2 million out of a 24 million population (4)) are banked (5). Yet, cell phone subscription in Africa rose from 54 million in 2003 to 350 million in 2008 with a forecast average cell phone penetration of 80 percent by 2012. Over 80% of Ghanaians have cell phones they can be identified with(6) (7). This has driven the gradual shift in Africa towards biometrics. The deployment of IdM systems is closely linked to electronic payment systems. The interplay between national IdM systems for citizen services and the commercial applications plays an important role for the deployment. However, this technological development has not come without challenges. There are several accounts of identity frauds, which have the potential of impeding the benefits of technological development in Africa. For instance, in Ghana, policy makers, security agencies and the private sector are bedevilled with cybercrime popularly known as "sakawa". Whereas "419" in Nigeria (8) has already become an international issue.

Implications on Technology Acceptance Model

Drivers of technology adoption and diffusion have been thoroughly studied and several theories and frameworks have been developed within Information Systems literature. Notable among them are innovation diffusion theory (9), technology acceptance model (TAM) (10) and the unified theory of acceptance and use of technology (UTAUT) (11). All of these theories are aimed at deepening understanding of the causal factors affecting technology adoption. In general, complexities, compatibility, relative advantage, ease of use and usefulness have been noted as some of the key drivers of technology adoption.

Particularly Davies, 1989 posit that the key factors influencing adoption are the perceived usefulness and perceived ease of use. Perceived usefulness describes the degree to which a person believes that the innovation will boost their performance, whereas perceived ease of use refers to the degree to which a person believes that adopting an innovation will be free of effort. Recently, these theories have been applied in digital IdMS (12), and this understanding has influenced the development of various e-IDM standards, guidelines and initiatives. These studies have mainly focused on developed countries. There are, however, other factors that are peculiar to developing countries, which is the focus of this paper.

The Era of Biometrics in Africa

Many western analysts perceive how third world countries can overtake the west by rapidly adopting emerging technologies as an awesome phenomenon (13). Throughout Africa, governments are moving towards biometric based national identity programs with the enactment of various acts of parliament. In Ghana, for instance, these include the payment systems ACT (ACT662) and national identification ACT (ACT 707)(14). As individuals become confident of who you are, and that they matter it acts as a step towards true freedom and self-actualisation(13). Biometric technologies are already allowing countries to achieve accurate census data and to use these numbers to drive informed policy formulation. This in turn leads to effective health and educational programme implementations, which drives investment and growth in the economy.

Identity Management Initiatives in Ghana

In Ghana, several independent IdM initiatives are under way. The National Health Insurance Scheme has already rolled out a nationwide registration by issuing identity cards to beneficiaries. The National Identification Authority is rolling out a biometric based national identification system, and the Ministry of Interior has introduced a biometric passport. Birth and death, voting, business registrations, social security, drivers and vehicle licensing are other forms of registrations performed by various government agencies in different formats and databases.

To enhance commercial activity and to reduce the unbanked and under-banked population in Ghana a biometric based payment system (e-zwich card) has been introduced by Bank of Ghana (BOG) (15). The system stores the fingerprint template on the chip embedded in the smart card as well on a central biometric server. The aim was to enable all e-zwich cardholders the ability to perform all transactions associated with traditional bank accounts such as; paying for goods and services, funds transfer, cash withdrawals, utility bill payments, and receiving salaries and pensions at any e-zwich points of sale (POS) terminals and Automatic Teller Machines (ATM) (16)]. According to France & Selormey, (2009) GhIPSS opted for biometric technology because of its superior security in terms of user authentication and its ability to combat card cloning. All commercial banks were directed to reconfigure their existing POS terminals and ATMs to make them e-zwich compatible (17).

Botswana

Previous studies in Botswana have shown that citizens trust the existing security systems used by organizations and for that matter there are no strong feelings of vulnerability that would warrant the adoption of biometric technology. In Botswana, the findings of (18) indicated that biometrics usage is at its infancy despite the fact that industries may be aware of its ability to strengthen security and productivity. Invariably somehow, these perceived benefits have had little effect on biometric technology adoption decisions. On the contrary, the critical adoption factors identified to be having an influence in Botswana were: Type and size of organization, Ease of use, and Communication or publicity campaign.

South Africa

The government of South Africa (Department of Home Affairs) embarked on Back Record Conversion Project in 2005 leading to the digitization of nearly 30 million hard-copy records of fingerprints and in its Home Affairs National Identification System (HANIS) database (19). With digital images of citizens' fingerprints, photographs and signatures, HANIS will enable the department to process citizens' national identification document applications electronically. The objective of the government was to eliminate manual, paper-based application processes. This speeds processing, is more accurate than a manual system, and costs less than alternatives. In addition to national ID cards and other government applications, biometrics has been used by the financial sector for some time, mostly for verifying identities and authenticating transactions.

Nigeria

The Nigerian government identified the need to integrate various Identity Schemes (IdS) into one effective and functional National Identity Management System (NIdMS) to complement its programme of social and economic reforms (20). The government believes this would provide a reliable system authentication and verification of citizens, promote e-government, boost national security, promote a reliable credit system, and minimise identity fraud. To foster transparency in elections the biometric based system will be used as the basis for compilation of "fresh voters" for the upcoming general election in 2011 and to update national census data. Several biometric based ATM cards have been introduced to combat ATM fraud which are mostly committed by individuals with connections with unscrupulous bank officials who able to provide pin numbers and other relevant information. Policy makers believe that it has the potential to eradicate ATM fraud.

IdM Adoption Survey in Ghana

In an attempt to gauge citizens perception on identification and payment systems, we conducted a survey using questionnaires and stakeholder interviews. The objective was to find out what influences their decision to adopt identification systems. A group of executive masters in administration participants were selected since they had come from various countries in West Africa and occupy various influential positions in both public and private sector. 250 questionnaires were administered and 230 responses were received and analysed. Interviewees were made up key officials from the National Identification Authority, E-ZWICH, the banks and trade merchants. The following key research questions were asked, what factors influence the implementation of IdMS and what factors determine commercial viability of such systems citizens adoption of electronic payment systems and what are factors. The following key constructs were used as criteria for measurement; perceived usefulness, perceived ease of use (10), commercial viability (21)(22), trusts and consequence of trust in the system(23).

Whereas National Identity (NID) Cards system encounter a lot of opposition in western countries, particularly US and United Kingdom, 90% of respondents believed that NID cards must be compulsory for all Ghanaians. Respondents had such faith in the system that they actually do not believe that the cards can be forged thereby destroying the integrity of the system. Another interesting findings was that majority of the respondents prefer that cards are issued to citizens free of charge. A further probe into this question through interview revealed varied explanations. Prominent among them were universal coverage and forgery prevention. Another interesting finding from the survey was that the respondents were unanimous in their responses questions on governance, policy and monitoring. For instance, they all believed that their interest would be considered in deciding how identity data is used. Additionally, the nation might not have enough competent personnel to manage the databases.

Even though security is a major concern to the western countries, in this survey respondents rather believed that the system will be secure and for that matter their personal data will not be affected even though they believed there are some risks involved. Concerning complexity in the use of the cards, majority of the respondents did not think it would be very difficult to use. A further probe however indicated that this believe stems from the fact respondents have all used ATM cards and thought the NID cards even in its advanced form may not be anything different. They also believed that introduction of the identity cards will not have any negative impact on users' personal information and that they were prepared to trade off some privacy for convenience, security and faster access to public service. Strangely, all the respondents were willing to allow identifications authorities to share their personal data with other government agencies and private businesses. A probe into the background of those not interested in national identification systems revealed that 90% were business people who felt the systems may be used for political witch-hunt and for tax purposes. Even though respondent felt that NID project is will promote feasible economic activity, they believed that the cards must be free.

Whereas National Identity (NID) Cards system encounter a lot of opposition in western countries, particularly US and United Kingdom 90% of respondents believed that NID must be compulsory for all Ghanaians. Respondense had such faith in the system that they actually do not believe that the cards can be forged thereby destroying the integrity in the system. Interestingly all the respondents somehow believed that forgery and fraudsters could undermine the usefulness the NID system since 100% of the respondents "ID cards will inevitably be forged which will undermine their effectiveness".

Another interesting findings was that majority of the respondents prefer that cards are issued to citizens free of charge. A further probe into this question in by way of interview revealed varied explanations prominent among the reasons were universal coverage and forgery prevention. Another interesting finding from the survey was that the respondents were unanimously in agreement with all three questions, regarding governance, policy and monitoring. For instance, they all believed that their interest would be considered in deciding how identity data is used. Additionally, they also thought we might not have enough competent personnel to manage the database.

Even though security was suppose to be of a major concern to citizens majority of the respondents rather believed that the system will be secure and for that matter their personal data will not be affected even though they believed there are some risks involved. Concerning complexity in the use of the cards, majority of the respondents did not think it would be very difficult to use. In addition, respondents do not think the identification agencies would encounter any difficulty in detecting fake ID cards. A further probe however indicated that this believe stems from the fact respondents have all used ATM cards and thought the NID cards even in its advanced form may not be anything different.

Respondents agreed to the notion that the identification system will allow government agencies to easily identify citizens and that in spite of the existing national ID systems (Voters ID Card, Driving Licence, etc). The caveat, however was that government must clearly explain all it reasons. Respondents felt they could rely on ID Authorities to work in their interest whenever there was a problem. They also believed that introduction of the identity cards will not have any negative impact on users' personal information. Virtually all the respondents were willing and prepared to trade off some privacy for convenience, security and faster response to public service. Strangely, all the respondents were willing to allow identifications authorities to share their personal data with other government agencies and private businesses. Even though respondent felt that NID project is economic feasible,

they believed that citizens must not be made for the issue of the ID cards.

Conclusion

This paper has identified factors influencing adoption of IdMS and its commercial viability in selected African Countries. It has also shown that security issues, privacy and anonymity, which are very critical to the adoption of IdMS in developed countries, are not the major concerns of those in developing countries. Rather, costs of equipment, tax implications, political issues, connectivity and compatibility with other payment systems were the key factors. In the case of e-zwich project in Ghana, each point of sale (POS) terminal is $700.00, which banks and merchants find it quite expensive whilst connectivity is not very good and adoption has not been very successful. In the same vein, perception of political motives, the use of the system for taxation purposes and free riding were seen as key factors that can inhibit the sustainability of the system. The paper has also confirmed (24) notion that introduction of technology by governments are often characterised by free riders, in the sense that different actors would like to use the system for their own benefit, but are not inclined to contribute to its maintenance. It is therefore important to find out measures that seek to strike a balance, which can be a topic for further research on IdMS in developing countries.

References

1. **Beynon-Davies, P.** (2007) 'Personal identity management and electronic government; the case of the national identity card in the UK,' *Journal of Enterprise Information Management*. Vol. 20, No.3, pp. 244-9.
2. **Seltsikas, Philip. and Heijden, Hans van der.** (2010) 'A taxonomy of government approaches towards online identity management', *Proceedings of the 43rd Hawaii International Conference on System Sciences*.
3. **OSGF** (2007) 'National Policy and Institutional Framework for an Identity Management System for Nigeria. Abuja, Nigeria', Abuja, Nigeria : Office of the Secretary to the Government of the Federation, The Presidency; [Online] http://www.nimc.gov.ng/public ations.html
4. **PMI (**2010) Country Profile: President's Malaria Initiative (PMI) Ghana, April.
5. **Amit, Jha., Neerajr, Negi. and Warria, Rekha.** (2007) *Ghana Microfinance Investment Environment Profile*.
6. **GBN.** (2010) 'Ghana's mobile penetration expected to hit 100% in 2013'. [Online] 2010. http://www.ghanabusinessnews.com/ [2010/06/08].
7. **Comninos, Alex., [et al.]** (2008) 'Towards Evidence-based ICT Policy and Regulation M-banking the Unbanked;' Policy Paper 4, IDRC. Vol.1.
8. **USDoS** (1997) 'Nigerian Advance Fee Fraud', s.l. United States Department of State Bureau of International Narcotics and Law Enforcement Affairs.
9. **Rogers, E.M.** (1993) 'Diffusion of Innovations', New York : The Free Press, 3rd edition.
10. **Davis, F. D.** (1989) 'Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology', *MIS Quarterly*, Vol. 13, No. 3, pp. 319-340.
11. **Venkatesh, V. and Davis, F.D.** (2000) 'A theoretical extension of the technology acceptance model: four longitudinal field studies', s.l. *Management Science*, Vol. 46, No. 2, pp. 186–204.
12. **Aichhlozer, Georg. and Strauß, Stefan.** (2009) 'Understanding a Complex Inovation process: Identity Management in Austrian E-Government', *The Proceedings of the 10th International Digital Government Research Conference*.
13. **Biometrics-in-Africa** (2009) 'The basis for the emergence of the individual' [Online] http://www. newstime.co.za/rs_articles_contributors.asp?conid=52& recid=752 25-09-2010 [October Friday, 23, 2009]
14. **NIA** National Identification Authority, (2010) *Editorial; NIA News*, April - June, Vol. 1.
15. **Frempong, Beatrice.** (2010) 'E-zwich is the dominant money transfer system in Ghana' [Online] www.Citifmonline.com [April Wed, 28th 2010], http://www.citifmonline.com/site/business/ news/view/5232/3.
16. **France, Fred. and Selormey, Dela**. (2009) 'Biometrics improving financial accessibility' *Biometric Technology Today*, July/August, pp. 10-11.
17. **Hesse, David Andreas.** (2009) 'The e-zwich electronic clearing and payment system', *Financial and corporate Ghana* 2009 Edition, s.l. www.iflr1000.com, p. 383.
18. **Uzoka, Faith-Michael. E. and Ndzinge, Tshepo.** (2009) 'Empirical analysis of biometric technology adoption and acceptance in Botswana', *The Journal of Systems and Software*, Vol. 82, pp. 1550–1564.
19. **Breckenridge, Keith**.(2005) Biometric Government in the New South Africa.
20. **Government of Nigeria** (2006) 'Harmonisation of National Identity Cards I.
21. **Tjan A.K.** (2001) 'Finally, a way to put your internet portfolio in order', *Harvard Business Review*, Vol. 79, No. 2, pp. 76-85.
22. **Liang T.P. [et al.]** (2007) 'Adoption of mobile technology in business: a fit-viability model', *Industrial management & data systems*, Vol. 107, No 8, pp. 154-169.
23. **FIDIS** Future of Identity in the Information Society: 'A Survey on Citizen's trust in ID systems and authorities', (2007).
24. Hardin, G. and Baden, J. (1977) *Managing the Commons*. San Francisco : Freeman.
25. **BTAM** Biometric Technology Application Manual (2008), 'Biometric Basics' ,[s.l] *National Biometric Security*.
26. **Aichholzer, Georg. and Strauß, Stefan.** (2009) 'The Citizens Role in National Electronic identity Management: A Case-study of Austria', *Second international Conference on Advances in Human-Oriented and Personalized Mechanisms, Technologies, and Services*, Porto, Portugal : s.n.
27. **Burger, Andrew. K.** (2010) Building the Case for Biometrics [Online] www.TechNewsWorld.com [Oct. 03/08/07 4:00, 2010].
28. **Cameron, K.** (2005) The Laws Of Identity [Online] identityblog. http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf [2005].

For further information please email adjei@cmi.aau.dk

biometrics

Exhibition and Conference 2011

Conference: 18–20 October 2011 | Exhibition: 19–20 October 2011

All the latest information and solutions on the use of biometric technology in government and commercial applications at Europe's premier event for biometrics.

INTERNATIONAL CONFERENCE

A topical overview of all the issues to consider when installing and operating a biometric system by international experts in the field.

MAJOR EXHIBITION

Free visitor access to the largest European exhibition for biometrics-based identity management solutions.

www.biometrics.elsevier.com

Strong ePassport verification in the private sector

By Michael Schwaiger
secunet Security Networks AG
and Aweke Lemma priv-ID B.V.

" ePassports might no longer be used for border controls alone but also for strong verification in the private sector. "

The need for strong identity checks

In recent years, an increasing number of services have become personalized. For these services to function properly, however, reliable identity (ID) verification methods are extremely important. To this end, in addition to systematic improvement of the quality of ID documents and the accompanying application and issuing processes, it is also vital to establish an undisputed relationship between the ID document and the person who holds it. The dramatic increase in so-called look-alike fraud in recent years shows that the traditional photo-based verification approach is not sufficient. This is why travel documents issued by European Union (EU) member states (see Council Regulation on biometrics in passports [EC]) and many other countries around the world include both a portrait photo and fingerprints in their electronic chip.

In Europe, institutions such as social services, employment agencies, banks and other financial bodies are legally required to verify the identity of citizens and clients. Even though these institutions could implement biometrics to carry out their regular ID checks, current European laws restrict the use of biometric information to authorized public authorities only. In particular, fingerprints stored in ID documents are protected from unauthorized use. This means that non-authorized institutions are forced to rely on the classic inspection-based ID verification procedures. Obviously, the reliability of an ID check could be significantly improved if the institutions could also perform biometric (that is, fingerprint) verifications. This would lead to a dramatic decrease in identity theft.

The Extended Access Control (EAC) protocol specified by the German Federal Office for Information Security (BSI), ensures that this data in the chip of the ID document is very well protected against unauthorized use. Using a Public Key Infrastructure (PKI) with digital certificates allows dedicated inspection systems to read out the fingerprint data. Apart from the current limitation to border checks, it can be assumed that the distribution and management of digital certificates will be insurmountable practical obstacles for actual wider use.

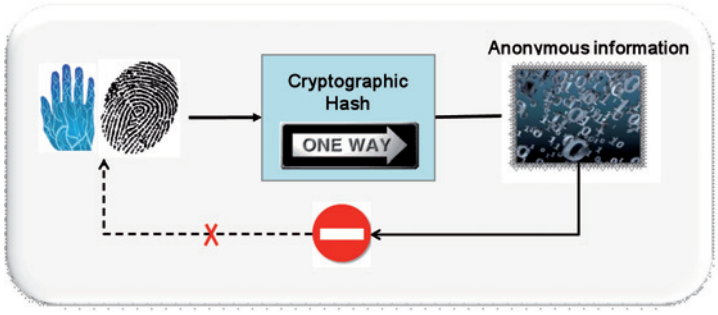
So, how can we grant the wish of numerous institutions to be able to use biometrics for ID checks within the framework of the mandatory privacy guarantees? The solution to this problem can be found in Privacy Enhancing Technologies (PET).

Privacy enhancing technology for biometrics

PET refers to technical measures that aim to safeguard and protect private data in information and communications solutions. It is preferably implemented as an integral part of the overall design choice. PET reduces the need for

complicated processes and procedures because it intrinsically enforces privacy. That is why it is also referred to as privacy by design. Furthermore, PET boosts the quality and transparency of information systems and enhances the citizen's or client's confidence in underlying services by addressing all privacy concerns.

One approach to PET is the so-called biometric template protection, in which a traditional biometric template is converted into an anonymous code. The conversion is based on a one-way function, also referred to as a cryptographic hash. By comparing the hash-codes, a reliable ID check can be carried out. Biometric features that are cryptographically hashed in this manner cannot be converted back into their original form. This means that the result can be referred to as an anonymous code and the information is no longer of a sensitive and personal nature. The following diagram illustrates the process.



The enrolment of biometrics for the benefit of this approach is the same as traditional enrolment. After taking the biometric data, it gets hashed resulting in an anonymous hash-code referred to as the anonymous template. The latter is then saved in the chip or register, depending on the application. Identity checks take place on the basis of comparing the recorded hash-code with a live measurement of the relevant biometric characteristic of the person, which gets hashed again during the verification process. If the hash saved in the chip or register matches the hash from the live measurement, the verification is positive.

Biometric template protection in ePassports

According to the definition of Machine Readable Passports in Doc 9303 [Doc9303-1] of the International Civil Aviation Organization (ICAO), the storage of electronic data on the chip of the travel document is managed by a Logical Data Structure (LDS). Consisting of several data groups (DGs), this structure ensures the global interoperability of travel documents. While personal data is stored in DG 1, DG 2 contains the digital portrait picture and DG 3 fingerprints of the document holder. Although, as defined by the ICAO, storing the fingerprint data in DG 3 is optional, the European Commission (EC) requires two fingerprints to be stored on passports issued within the EU. Optionally, iris images can be stored in DG 4.

Securing the data on the chip, DG 1 and DG 2 are protected by a basic security mechanism – the Basic Access Control (BAC) protocol [Doc9303-3], which is mainly based on secure messaging with session keys derived from the optically scanned Machine Readable Zone (MRZ) of the travel document. Further protocols ensure the integrity of the data on the chip and that it is genuine. However, within the EU, fingerprints stored in DG 3 (and iris images stored in DG 4) have to be protected by stronger mechanisms which are described in the EAC specification [EAC]. This includes Terminal Authentication (TA) and Chip Authentication (CA) in addition to all the other procedures defined by the ICAO [Doc9303-3]. Besides the mentioned mandatory data groups for ePassports issued within the EU, DG 13 is an optional data group and can be used for optional details. It is up to the issuing country of the passport if and what data is stored in DG 13.

An anonymous biometric template (as mentioned in the previous section) of the holder of the document could be stored as optional details in this DG 13. During personalization of the passport, an anonymous template of any biometric feature of the document holder is generated and stored on the chip. Unlike DGs 3 and 4, where fingerprints and iris are stored as digital images, the anonymous biometric template needs no further access protection because it is protected by the privacy enhancing technology used for biometric data. As a result, only the BAC protocol needs to be performed during the verification process to access the stored anonymous biometric template in DG 13. It may then be used as a reference for comparing it with the template extracted from the query image and performing a verification of the document holder.

The main advantage of this solution is that biometric verification (that is, fingerprint or iris) can be applied without having to perform the full EAC protocol including the setup of a national Country Verifying Certification Authority (CVCA) and the sub-components needed to perform the Terminal Authentication (TA) protocol (see [EAC] for further information). This means that PET offers a unique opportunity for private authorities to use strong biometric verification together with secure ePassports in scenarios other than border control.

In a prototype implementation, secunet Security Networks AG and priv-ID B.V. have developed a solution for using privacy enhancing fingerprint technology in private sector ID verifications. It is integrated into the reference architecture for reading electronic travel documents – the Golden Reader Tool Platinum Edition [GRT, GRT-PE] developed by the German BSI and secunet. It demonstrates how to use fingerprint template protection algorithms for identity checks with ePassports.

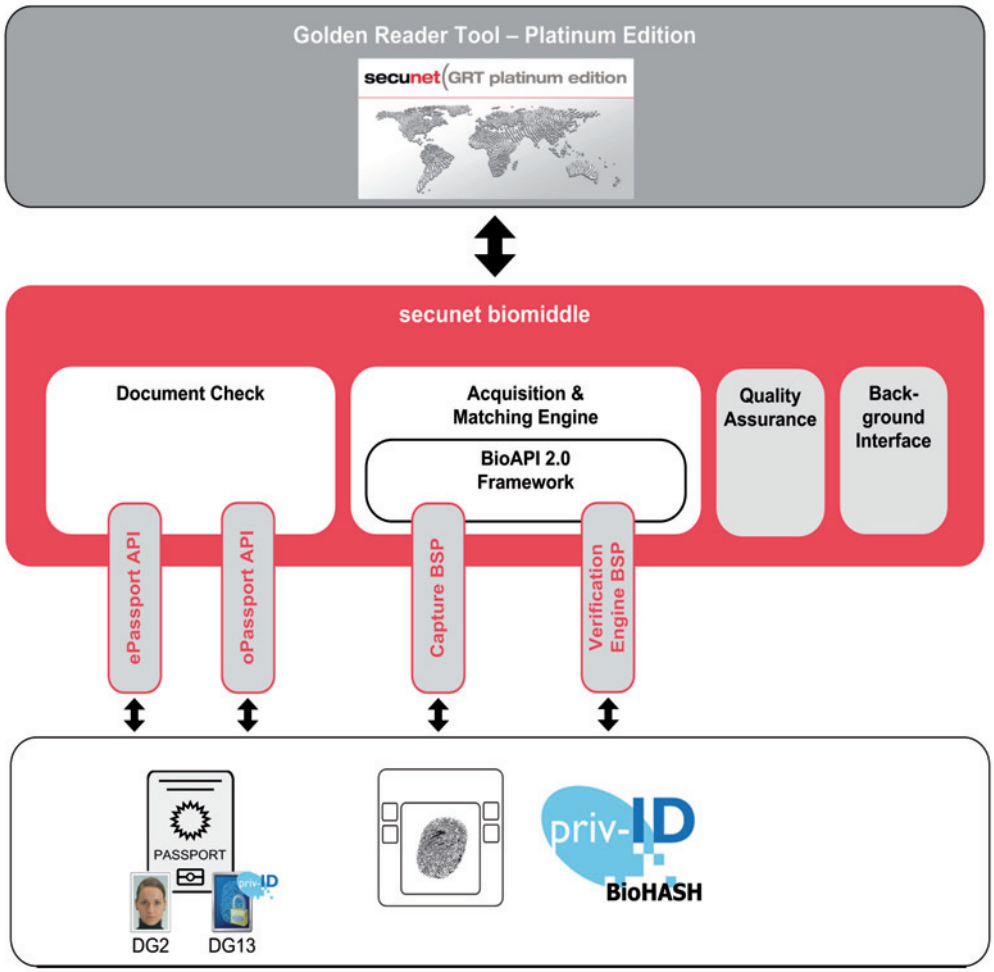
The architecture of the prototype implementation is based on the biometric middleware, secunet biomiddle [biomiddle], which is a layer between the application and all biometric and electronic hard- and software. The following illustration shows the architecture design.

Using the integrated ePassport API, anonymous fingerprint data stored during the passport personalization process is read out from DG 13 and returned to the application – the Golden Reader Tool. In order to check the identity of the passport holder, the integrated BioAPI 2.0 framework [BioAPI2.0] is used to capture a query fingerprint. This is realized by using a compliant Capture Biometric Service Provider (BSP) which addresses the connected fingerprint device. The identity check itself is performed by a Verification Engine BSP which implements the actual biometric template protection algorithm. In this demonstration, the privacy protecting fingerprint algorithm BioHash from priv-ID B.V. is used to verify the identity of the document holder. The results of the identity check are then displayed in the Golden Reader Tool's user interface in addition to all the security checks that have been performed on the electronic passport.

Through the modular architecture of secunet biomiddle and the underlying BioAPI 2.0 framework, an exchange of the biometric template protection algorithm would be possible by just using different BSPs for verification. Due to a lack of exchange format standards for biometric template protection approaches, it would even be possible to select the appropriate verification algorithm independent of the algorithm used for creating the anonymous reference template during passport production. The information indicating which version of which algorithm is used for preserving the privacy of the biometric data is also stored in DG 13.

New possibilities for private sector verifications

The prototype demonstration shows that it is possible to use privacy enhancing technology for biometrics-based identity checks in conjunction with electronic travel documents. ePassports might no longer be used for border controls alone but also for strong verification in the private sector. Banks could use this sort of identity check for customers opening a bank account or withdrawing money. Social services could



use strong identity checks to prevent misuse of the services they offer. And countries outside the EU could use this approach for border control as well. They could avoid having to implement, set up and maintain an expensive PKI for protecting sensitive biometric data electronically stored on national ID documents.

To enable these possibilities, privacy enhancing technologies for biometric data need to be developed and implemented worldwide. This is not yet the case. But what we can say for sure is that template protection safeguards the security and privacy of biometric data, especially when it is used for strong verification in the private sector.

References

[EAC] German Federal Office for Information Security (BSI) – *Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI)*. 2010. Version 2.04.

[Doc9303-1] International Civil Aviation Organization (ICAO) – *Machine Readable Travel Documents. Part 1 Machine Readable Passports. Volume 2 Specifications for Electronically Enabled Passports with Biometric Identification Capability.* 2006. Sixth Edition.

[Doc9303-3] International Civil Aviation Organization (ICAO) – *Machine Readable Travel Documents. Part 3 Machine Readable Official Travel Documents. Volume 2 Specifications for Electronically Enabled MRtds with Biometric Identification Capability*. 2008. Third Edition.

[GRT] German Federal Office for Information Security (BSI) - Webpage *Golden Reader Tool*: https://www.bsi.bund.de/cln_174/DE/Themen/ElektronischeAusweise/Projekte/projekteGRT/GRT_node.html

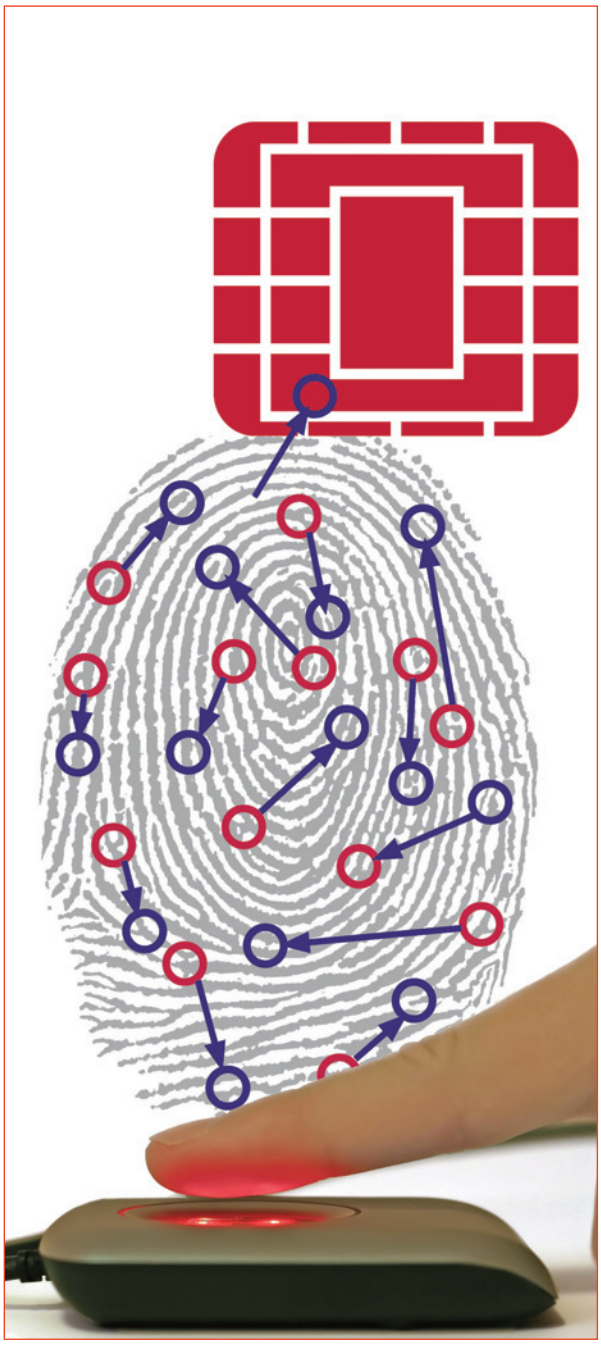
[GRT-PE] secunet Security Networks AG – Webpage *secunet GRT – Platinum Edition*: http://www.secunet.com/de/produktedienstleistungen/government/biometrie-hoheitliche-dokumente/grt-platinum edition/

[BioAPI2.0] ISO/IEC 19784-1:2006 - *Information technology – Biometric application programming interface – Part 1: BioAPI specification*. 2006. First edition.

[biomiddle] secunet Security Networks AG – Webpage *secunet biomiddle*: http://www. secunet.com/en/products-services/government/biometrics-eids/secunet-biomiddle/

[EC] European Commission - *Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States*. 2004. URL: http://eur-lex.europa.eu/LexUriServ/ LexUriServ.do?uri=CELEX:32004R2252:EN:HTML

For further information please email michael.schwaiger@secunet.com or visit www.secunet.com or email aweke.lemma@priv-id.com or visit www.priv-id.com

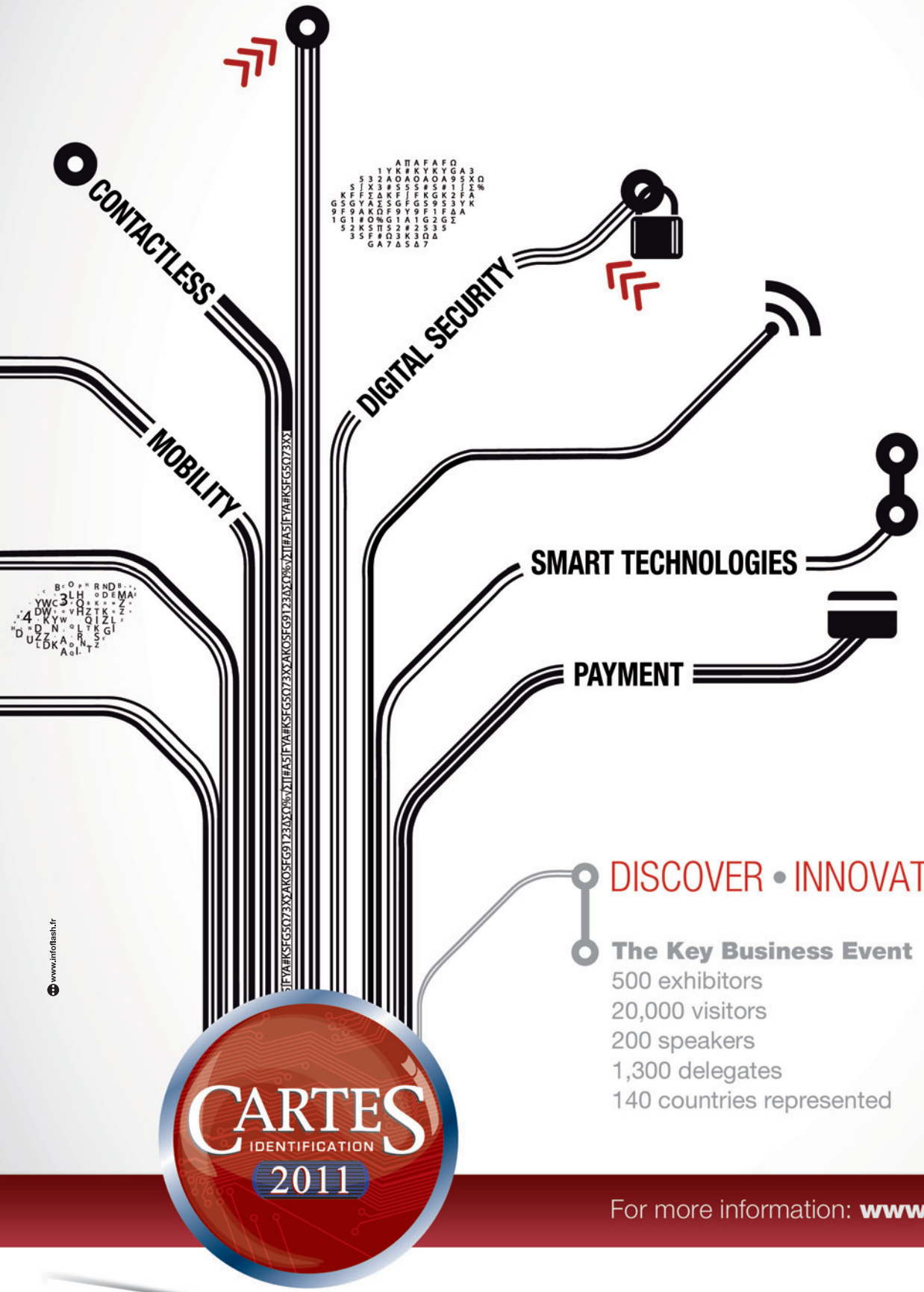


EXHIBITION & CONFERENCES

CARTES & IDentification

15 - 16 - 17 November 2011

Paris Nord Villepinte Exhibition Center - France



DISCOVER • INNOVATE • DEVELOP

The Key Business Event

500 exhibitors
20,000 visitors
200 speakers
1,300 delegates
140 countries represented

For more information: **www.cartes.com**

An event organized by comexposium

Country guest of honour

ASSOCIATIONS

Advanced Card Technology Association of Canada

ACT Canada is the stakeholder association, focused on secure payment, secure identity management and other advanced applications. We are the authority on the Canadian market, supporting our members through working with key stakeholders. We help members understand the market, public and private sector applications and potential barriers. We facilitate knowledge transfer and thought leadership through a neutral forum, while expanding our members' networks. Founded in 1989, ACT Canada is a non-profit membership association.

Web: www.actcda.com

Association for automatic identification and mobility

Since 1972, AIM has actively led the way in industry standards, education, and outreach.

AIM is the international trade association representing automatic identification and mobility technology solution providers. Through the years, industry leaders continue to work within AIM to promote the adoption of emerging technologies.

AIM actively supports the development of AIM standards through its own Technical Symbology Committee (TSC), Global Standards Advisory Groups, and RFID Experts Group (REG), as well as through participation at the industry, national (ANSI) and international (ISO) levels.

Web: www.aimglobal.org

The Biometric Consortium

The Biometric Consortium serves as a focal point for research, development, testing, evaluation, and application of biometric-based personal identification /verification technology. The Biometric Consortium organizes a premier biometrics conference

Web: www.biometrics.org

Biometrics Institute

The Biometrics Institute is the independent not-for-profit user group with currently over 100 member organisations including government departments, financial services institutions, health service providers and also vendors of biometric products and services. It is THE meeting place for organisations who have an interest in biometrics and would like to share experiences and receive information and training in an informal environment. The Biometrics Institute is based in Australia.

Web: www.biometricsinstitute.org

The European Biometrics Forum

The European Biometrics Forum is an independent European organisation supported by the European Commission whose overall vision is to establish the European Union as the World Leader in Biometrics Excellence by addressing barriers to adoption and fragmentation in the marketplace. The forum also acts as the driving force for coordination, support and strengthening of the national bodies

Web: www.eubiometricsforum.com

European Campus Card Association

ECCA is a non-profit educational association that works to provide learning and networking opportunities for campus ID card and card industry professionals. The association offers a newsletter website, an annual conference, and regional workshops on topics related to campus cards.

Web: www.ecca.ie

EUROSMART

EUROSMART is an international non-profit association located in Brussels representing the Voice of the Smart Security Industry for multi-sector applications. Since its creation in 1995, Eurosmart is committed to expanding the world's smart secure devices market, developing smart security standards and continuously improving quality and security applications. Smart Secure devices are smart objects which contains a secure IC and embedded software and support personalization by the issuer. The main purpose is to offer Human to Machine as well as Machine to Machine security services such as data integrity, user authentication or secure storage. It comes in multiple form factors, including Smart card and Smart USB token. This includes personal, portable as well as embedded devices.

Web: www.eurosmart.com

Intellect

Intellect provides a collective voice for its members and drives connections with government and business to create a commercial environment in which they can thrive. Intellect represents over 750 companies ranging from SMEs to multinationals. As the hub for this community, Intellect is able to draw upon a wealth of experience and expertise to ensure that our members are best placed to tackle challenges now and in the future.

Web: www.intellectuk.org

National Association of Campus Card Users

NACCU was formed in 1993 to provide a responsive, diversified source of campus card related information and services. NACCU membership is open to all colleges, universities, secondary institutions and companies that are involved with the campus card market.

Web: www.naccu.org

The Silicon Trust

The Industry's Benchmark Silicon Based Security Partner Program.

Since the year 2000, when the Silicon Trust was founded by Infineon Technologies as a marketing program for smart card solutions, the program has developed to be a key partner platform for companies aiming at promoting the use of silicon-based security in a broad variety of applications including Identification, Telecom and Payment. With more than 20 active member companies in 2008, Silicon Trust now forms a strong community of like-minded companies. Today, the driving force behind the Silicon Trust are the three executive partners: Gemalto, Giesecke & Devrient and Infineon Technologies, supported by the German Federal Office for Information Security (BSI) in the Silicon Trust advisory board. Many other companies along the value chain of silicon-based security participate in Silicon Trust discussions and activities.

Web: www.silicon-trust.com

Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America.

Smart Card Alliance Identity Council

The Smart Card Alliance Identity Council is focused on promoting the need for technologies and usage solutions regarding human identity information to address the challenges of securing identity information and reducing identity fraud and to help organizations realize the benefits that secure identity information delivers. The Council engages a broad set of participants and takes an industry perspective, bringing careful thought, joint planning, and multiple organization resources to bear on addressing the challenges of securing identity information for proper use.

Web: www.smartcardalliance.org

Smart Card Forum of China

SCFC is a non-governmental and non-profit, multi-vendor and end-user society, supported by manufacturers, suppliers, institutions, organizations and individuals as well as the corporate societies etc. in the smart card industry, which promotes the smart card industry and the value of its products and services while providing an independent forum to speak for the industry in China.

Web: www.scfc.org.cn

Smart X Central Intelligence

Smart x central intelligence operates within an international network of professional associations concerned with smart card and RFID technologies, and related emerging technologies. World membership exceeds 500 companies in the UK, Africa and the Asia Pacific regions.

Smart x is the only professional association for the industry covering Southern Africa, with members in the major business centres of the country. Smart x membership is represented by private and public sector end-users, solutions providers and consultants that receive

real benefits from the associations' active participation in the industry. The aim of smart x is to make its members aware of the developments taking place in the industry both in South Africa and internationally.

Web: www.smartx.co.za

Smartex Limited

Smartex Limited operates an international network of professional associations concerned with smart card and RFID technologies, and the UK Purchasing Card market. World membership exceeds 500 companies in the UK, Africa and the Asia Pacific regions:
Smartex also provides a range of independent consultancy, project management and systems integration services relating to citizens' card schemes for Local Authorities, and campus card schemes for universities.

Smartex forums

Smart Card Club
International Biometric Foundation
Transport Card Forum
Smart Government Forum
Higher Education Smart Card Assoc.
EuroTag
Purchasing Card Forum

Web: www.smartex.com

STANDARDS

GlobalPlatform, Inc.

GlobalPlatform is the international specification body for smart card infrastructure. GlobalPlatform aims to maintain and drive adoption of its technical specifications which provide an open and interoperable infrastructure for smart cards, devices and systems. The GlobalPlatform smart card infrastructure is intended to simplify and accelerate deployments that support multi-application, multi-actor and multi-business model implementations.

Web: www.globalplatform.org

Integrated Transport Smart card Organisation

Incorporated in 2001, ITSO is a non-profit distributing organisation, whose membership covers the breadth of the Transport arena including transport operators, suppliers to the industry, local authorities and public transport executives. Supported by the Department for Transport, ITSO has links with major transport industry organisations and established smartcard schemes in the UK and overseas.
Having evolved from the initiative of various UK Passenger Transport Authorities who were concerned with the lack of standards for interoperable smartcard ticketing ITSO started in 1998. ITSO's objective is to maintain and develop the ITSO Specification; to operate and manage an interoperable smart media environment and to facilitate and support development of interoperable smart ticketing schemes that comply with the ITSO Specification.

Web: www.itso.org.uk

Java Card Forum

The primary purpose of the Java Card Forum is to promote and develop Java as the preferred programming language for multiple-application smart cards. Java, invented by Sun Microsystems in 1995, has important features that make it the ideal choice for smart cards.

Web: www.javacardforum.org

MAOSCO Ltd.

MULTOS is a trademark of MAOSCO Ltd. MULTOS is an open, non-proprietary, all inclusive smart card operating system. To ensure its openness and to further advance its adoption into all smart card related markets, the control of the MULTOS specification is contractually invested in The MULTOS Consortium. The MULTOS Consortium is also known as MAOSCO and MAOSCO Limited is the legal name of the secretariat company.

Web: www.multos.com

SMART CARD CENTRE

ISG-Smart Card Centre, Royal Holloway University of London

The Smart Card Centre was founded in October 2002 by Royal Holloway University of London, Vodafone and Giesecke & Devrient.
The primary objective was to create a World-Wide centre of Excellence for training and research in the field of Smart Cards, applications and related technologies.
It is a testimony to the world-wide reputation of Royal Holloway's Information Security Group, that the largest Mobile Operator in the world and one of the largest global card manufacturers, chose to found the Centre at Royal Holloway

Web: www.scc.rhul.ac.uk

COMPANIES

3M Security Systems
Corporate Headquarters
3M Center St. Paul,
Minnesota
MN 551441000
USA
Tel: +1 888 364 3577
Email: lcole1@mmm.com
Web: www.3m.com
Manufacturing & Personalisation,
Identification & Authentication
solutions, ID smartcards

A

A.R. Hungary, Inc.
Kiralyhago ter 8-9
Budapest 1126
Hungary
Tel: +36 1 20 19 650
Email: requestinfo@arhungary.hu
Web: www.arhungary.hu
Readers & Terminals, e-Passport
Reader

Abacicard San, Tic AS
Seyrantepe,
Çelik Cad. No: 69/2
34418 4 Levent
Istanbul
Turkey
Tel: +90 212 324 34 00
Email: info@abacicard.com
Web: www.abacicard.com
Manufacturing & Personalisation,
ID smartcards

Abnote
American Banknote Corporation
2200 Fletcher Avenue
Fort Lee,
NJ 07024
USA
Tel: +1 201-592 3400
Web: www.abnote.com
Manufacturing & Personalisation
ID smartcards, ePassports
Personalisation Systems & Software

Aceprox Identifikations-Systeme
Bahnhofstrasse 73
Helpsen, D-31691
Germany
Tel: +49 5724 98360
Email: info@aceprox.de
Web: www.aceprox.de
Manufacturing & Personalisation
Readers &Terminals

ACIG AG
Erthalstraße 1
Bonifaziusturm B.
Mainz, D-55118
Germany
Tel: +49 6131 62994 0
Email: aw@acig-ag.com
Web: www.acig-ag.com
Manufacturing & Personalisation

Aconite Technology Ltd.
8 - 14 Vine Hill
London, EC1R 5DX
UK
Tel: +44 20 7713 4800
Email: contactus@aconite.net
Web: www.aconite.net
Manufacturing & Personalisation,
Card test tools, ID smartcards,
e-tickets, ePassports

Actividentity Corp.
6623 Dumbarton Circle
Fremont
CA 94555
USA
Tel: +510 574 0100
Email: info@actividentity.com
Web: www.actividentity.com
Identity authentication and credential
management solutions

Adaptive Recognition Hungary
Kiralyhago ter 8-9
1126 Budapest
Hungary
Tel: +36 1 20 19 650
Email: inforeqst@arhungary.hu
Web: www.passport-reader.com
Readers & Scanners

Adel SRl
Via Nonantolana n. 970/1
41122 Modena
Italy
Tel: +39 059 2550137
Email: adel@adel2000.it
Web: www.adel2000.it
Card Personalisation machinery

ADI Kartes Ltd
Kr.Barona 7/9-20,
Riga LV 1050,
Latvija
Tel: +371 672 95 420
Email: kartes@adikartes.lv
Web: www.adikartes.lv
Produce & Personalise Cards

ADT Security Systems
3601 Eisenhower Avenue
Alexandria
VA 22304
USA
Tel: +1 703 317 4200
Email: mflannery@adt.com
Web: www.adt.com
Access Solutions & ID Systems
Security & RFID

Advanced Card Sytems Ltd
Units 2010-2013, 20th Floor
Chevalier Commercial Centre
8 Wang Hoi Road,
Kowloon Bay
Hong Kong
Tel: +852 2796 7873
Email: info@acs.com.hk
Web: www.acs.com.hk
Manufacturing & Personalisation,
ID smartcards

AdvanIDe GmbH
Am Klingenweg 6A,
65396 Walluf,
Germany
Tel: +49 6123 791 400
Email: info@aaitg.com
Web: www.advanide.com
Manufacturing & Personalisation
Readers & Terminals, ID &
Authentication, eToken

AGFA - Gevaert N.V.
Septestraat 27
Mortsel B 2640
Belgium
Tel: +32 3 444 2111
Web: www.agfa.com
Manufacturing & Personalisation
ID cards

AGYS
4 avenue Sébastopol
BP 95204 57076
Metz Cedex 3
France
Tel: +33 825 120 999
Email: info@agys.fr
Web: www.agys.fr
Personalisation Systems

Aladdin Knowledge Systems
SafeNet
4690 Millennium Drive
Belcamp, MD 21017
USA
Tel: +1 410 931 7500
Email: orders@safenet-inc.com
Web: www.aladdin.com
Manufacturing & Personalisation
ID & Authentication, eToken, ID smartcards

Alios
Zone Neptune II
50008 Saint-Lô
France
Tel: +33 2337 76565
Email: contact@alios-card.com
Web: www.alios-card.com/
Card Manufacturing & Personalisation
Personalisation Systems & Software

AllStar Card Systems
5220 Spring Valley Rd 200
Dallas,
Texas 75254
USA
Tel: +1 800 290 0463
Email: sales@allstarcardsytems.com
Web: www.allstarcardsystems.com
ID card printers, ID card software, Card based solutions

Antheus Technology Inc.
22241 Larkspur Trail
Boca Raton
FL 33433
USA
Tel: +1 561 459 4813
Email: help@antheustechnology.com
Web: www.antheustechnology.com
Fingerprint Identification Software

ARE CON GmbH & Co. KG
Fliederweg 5
D-26209 Hatten
Germany
Tel: +49-441-8000 676
Web: www.are-con.com
Consultancy, ID products solutions

Arjowiggins Security
Immeuble Axe Seine
20, rue Rouget de Lisle
92130 Issy les Moulineaux Cedex
France
Tel: +33 1 41 08 60 00
Email: security@arjowiggins.com
Web: www.arjowiggins.com
ID & authentication solutions

Arnold GmbH
Mörfelder Landstrasse 11
D 63225 Langen
Germany
Tel: +49 610379023
Email: twa@cardcontrol.com
Web: www.cardcontrol.com
Readers & Terminals, Access control ID cards

ASK
2405 route des Dolines
06560 Sophia Antipolis
France
Tel: +33 4 97 21 40 00
Email: info@ask.fr
Web: www.ask-rfid.com
Contactless microprocessor smart cards & Smart Paper ID solution

Athena Smartcard Solutions
1-14-16, Motoyokoyama-cho
Hachioji-shi
Tokyo, 192-0063,
Japan
Tel: +81 426 60 7555
Email: sales@athena-scs.com
Web: www.athena-scs.com
Manufacturing & Personalisation
Readers & Terminals, ID cards

ATLANTIC ZEISER GmbH
Bogenstraße 6-8
78576 Emmingen
Germany
Tel: +49 7465 291 0
Email: sales@atlanticzeiser.com
Web: www.atlanticzeiser.com
Manufacturing & Personalisation

Aurora Technologies Ltd
1 Etgar Street,
Tirat Carmel 30200
Israel
Tel: +972 4 8576982
Email: info@aurora.co.il
Web: www.aurora.co.il
Card Personalisation

Authenti-Corp
PO Box 51675
Phoenix,
Arizona 85076
USA
Tel +1 480 889 6400
Email: info@authenti-corp.co
Web: www.authenti-corp.com
Personal authentication solutions
ID documents

Autofeeds
2726 Summerset Circle
Suamico
WI 54173
USA
Tel: +1 920 434 9808
Email: sales@aol.com
Web: www.autofeeds.com
Laminated National ID & Security products

Avalon Biometrics SL.
Calle de Basauri 17
Edf.B, Ofc.F
28023 Madrid
Spain
Tel: +34 91 70 80 5 80
Email: info@avalonbiometrics.com
Web: www.avalonbiometrics.com
ID solution provider

Aventra Oy
Lanttikatu 2
FIN-02770 ESPOO
Finland
Tel: +358 9 4251 1251
Email: sales@aventra.fl
Web: www.aventra.fi
Manufacturing & Personalisation, Smart cards, Data security

Aware, Inc.
40 Middlesex Turnpike
Bedford,
MA 01730,
USA
Tel: +1 781 276 4000
Email: info@aware.com
Web: www.aware.com
Manufacturing & Personalisation, Encoding technologies, & Secure credential applications

Axode
ZAC de la Petite Camargue
352 Chemin des Oliviers
34400 Lunet
France
Tel: +33 4 67 66 70 50
Email: sales@axode.com
Web: www.axode.com
Security Systems & Identification Engineering

B

Bayometric
1743 Park Avenue,
San Jose,
CA 95126
USA
Tel: +1 877-917-3287)
Email: sales@bayometric.com
Web: www.bayometric.com
Biometric security solutions, fingerprint, face, iris, & voice

B-Id GmbH & Co., KG
Von-Seebach-Strasse 28
D-34346 Hannoversch Muenden
Germany
Tel: +49 5541 95 66 70
Email: info@b-id.eu
Web: www.b-id.eu
Manufacturer of RFID products, Readers & Terminals

Bell ID
Stationsplein 45
Unit A6.002
3013 AK Rotterdam
The Netherlands
Tel: +31 10 885 1010
Email: info@bellid.com
Web: www.bellid.com
ID & ePassport security solutions, ANDiS Management System

BG Ingénierie
4 rue Paul Langevin,
ZAC de la Goulgatière,
35220 Chateaubourg
France
Tel: +33 2 99 00 89 97
Fax:: +33 2 99 00 89 98
Email: information@bginge.com
Web: www.bginge.com
Card testing

Bilcare Technologies

Bilcare Technologies
Malvern Hills Science Park,
Geraldine Road,
Malvern, WR14 3SZ,
UK
Tel: +44 (0) 1684 585 257
Email: tech@bilcare.com
Web: www.bilcaretech.com
ID credential and document security & anti-counterfeiting

Bilcare Technologies is a research and technology leader focused on next-generation anti-counterfeiting, security and brand protection solutions for a broad range of industrial applications including documents, financial instruments and identification credentials. We are part of the Bilcare Group, a global company that also provides advanced packaging solutions and tailored clinical trial services. Our flagship anti-counterfeiting and security product nonClonableID™ enables documents, cards and packaging to be uniquely serialized and authenticated in real-time by a variety of stakeholders including inspectors, security organizations and end-users. Our solution is also compatible with various access control systems and existing document formats. Our approach is to provide customers with tailored solutions; selected and customized from our range of products and services. We have technical and business teams located around the world, including the UK, mainland Europe, US, India and Singapore.

Bio-Key International
Allaire Corporate Center
3349 Highway 138
Building D Suite A
Wall, NJ 07719
USA
Tel: +1 732 359 1100
Email: information@bio-key.com
Web: www.Bio-key.com
Biometric Solutions

Bion Biometrics Inc.
38 Summerwind Crescent
Nepean,
Ontario K2G 6G5
Canada
Tel: 613-823-8928
Web: www.bionbiometrics.com
Biometric standards and systems

BÖWE CARDTEC
Balhorner Feld 28
Paderborn D-33106
Germany
Tel: +49 5251 18086 0
Email: info@boewe-cardtec.de
Web: www.boewe-cardtec.com
Manufacturer of modern high-performance cutting and inserting systems, Solutions provider

Bundesdruckerei GmbH
Oranienstrasse 91
D-10969 Berlin
Germany
Tel: +49 30 25 98 2414
Email: info@bundesdruckerei.de
Web: www.Bundesdruckerei.de
Biometric & Authentication Solutions, ID cards, Biometric Smart Cards

C

CanCard
177 Idema Road
Markham
Ontario L3R 1A9
Canada
Tel: +1 416 449 8111
Email: sales@cancard.com
Web: www.cancard.com
Card Printing & Card Personalisation Systems

Card Personalisation Solutions Ltd.
Unit 2 The Bramery
44 Alstone Lane
Cheltenham
Gloucestershire GL51 8HE,
UK
Tel: +44 0845 130 0240
Email: info@cardps.co.uk
Web: www.cardps.com
Card Personalisation Solutions

Cardag Deutschland GmbH
An der Allee 6
D-99848 Wutha-Farnroda
Germany
Tel: +49 36921 30 70
Email: info@cardag.de
Web: www.cardag.de
Manufacturing & Personalisation, ID contactless and contact smart cards

CardLogix
16 Hughes, Suite 100
Irvine, CA 92618
USA
Tel: +1 949-380-1312
Web: www.cardlogix.com
Smart card personalisation

Cartiere Miliani Fabriano SpA
Viale Pietro Milani 31/33
60044 Fabriano (AN)
Italy
Tel: +39 0732.7021
*Email:*mail@cartieremiliani fabriano.com
Web: www.cartieremilianifabriano.com
Security paper documents, Security printing

Cartoplast
13, rue de Colmar
68153 Rineauxe Cedex
France
Tel: +33 3 89 73 29 73
Fax: +33 3 89 73 29 72
Email: commercial@cartoplast.fr
Web: www.cartoplast.fr
Personalisation

CBN ID Systems Division
18 Auriga Drive
Ottawa,
Ontario K2E 7T9
Canada
Tel: +1 613 7226607
Email: identification@cbnco.com
Web: www.cbnco.com/corp
Identification Systems / Security-printed products

C&C RFID (Shanghai) Co., Ltd.
Room 303,
29, Lane 165,
Fangfa Mansion,
Dong Zhu An Bang Road,
Shanghai 200050
China
Tel: 86 21 52381295
Web: www.rfidcandc.com
RFID ePassports

Cea Leti
17, rue des Martyrs
38054 Grenoble cedex 9
France
Tel: +33 4 38 78 44 00
Web: www.cea.fr
Information, Research, & Technology Resource Centre; Contactless and secure chip design; Readers & Terminals

Centro Grafico DG
via Einstein, 76
20010 Marcallo (MI)
Italy
Tel: +39 02 - 9761301
Email: info@centrograficodg.it
Web: www.centrograficodg.it
Security printing, holographic film & foils´ production technology

Certego GmbH
Lichtenbergstrasse 8
85748 Garching
Germany
Tel: +49 89 360 55 370
Email: info@certego.com
Web: www.certego.com
Biometrics for ID Cards & High Security Access Control

CETECOM ICT
Unterturkheimer Strasse 6 -10
66117 Saarbrucken
Germany
Tel: +49 681 598 0
Email: info@ict.cetecom.de
Web: www.cetecom-com
Readers & Terminals, Testing

CFC International
500 State Street
Chicago Heights
IL 60411
USA
Tel: +1708 891 3456
Email: cfcinfo@cfcintl.com
Web: www.cfcintl.com
Holographic Security & Authentication Solutions

Chanwanich Security Printing Co., Ltd.
Kongboonma Building
699 Silom Road
Bangrak
Bangkok 10500
Thailand
Tel: +66 2635 3355
Email: marketing@chanwanich.com
Security printing, Identification doc.
Web: www.chanwanich.com

China Vision Intelligence & Techn. Co.
D-901, Shenzhen Academy of Aerospace Technology,
10 Kejinan Road
High Tech Zone
Nanshan District
Shenzhen Gangdong
518057 Shenzhen
China
Tel: +86 755 8611 7608
Email: info@cv-it.com
Web: www.cv-it.com
Biometric Solutions, Smart Card Readers

ChipCard Solutions GmbH
Muehlweg 2a
82054 Sauerlach
Germany
Tel: +49 (0)8104 629 34-0
Email: info@chipcard-solutions.com
Web: www.chipcard-solutions.com
Consultants, chipcard and RFID solutions

CIM S.p.A.
Loc. Braine, 54/A
40036 Rioveggio
Bologna
Italy
Tel: +39 051 67 76 611
Email: info@cimitaly.it
Web: www.cimitaly.it
Card Manufacturer & Personalizing

Cogent Systems
639 N. Rosemead Blvd.
Pasadena, CA 91107
USA
Tel: +1 626 325 9600
Email: info@cogentsystems.com
Web: www.cogentsystems.com
biometric identification systems

Cognitec Systems GmbH
Grossenhainer Str. 101, Tower B
D-01127 Dresden,
Germany
Tel: +49 351862 920
Web: www.cognitec-systems.de
Face recognition technology for border control, passport or drivers' license issuance

Collis B.V.
De Heyderweg 1
2314 XZ Leiden
The Netherlands
Tel: +31 71 581 36 36
Email: info@collis.nl
Web: www.collis.nl
e-Identification testing tools for card issuers, personalisers and test labs

Consult Hyperion
Tweed House 12 The Mount
Guildford, Surrey GU2 4HN

UK
Tel: +44 1483 301793
Email: info@chyp.com
Web: www.chyp.com
Consultancy, identity management, electronic transactions

Corestreet
One Alewife Center, Suite 200
Cambridge,
MA 02140
USA
Tel: +1 617 661 3554
Email: info@corestreet.com
Web: www.corestreet.com
ID & Authentication, Access control

Compass Plus
68, Prospect Lenina,
Magnitogorsk, 455044,
Russia
Tel: +7 495 502 9922
Email: enquiries@compassplus.com
Web: www.compassplus.com
TranzWare card personalisation solutions

Cross Match Technologies GmbH
Unstrutweg 4
07743 Jena
Germany
Tel: +49 3641 4297-0
Fax: +49 3641 4297 41
Email: international-sales@crossmatch.com
Web: www.crossmatch.com
Biometric identity management systems, fingerprint, palm solutions

Cross Match Technologies is a leading global provider of high-quality interoperable biometric identity management solutions.

The company offers fingerprint, palm scan and facial recognition systems, enterprise and application software, document readers, dual iris scanners, and related services. These products are used in markets such as national, state and local governments, law enforcement, financial services, transportation, education, healthcare, and others.

Cryptography Research
575 Market Street, 11th Floor
San Francisco
CA 94105
USA
Tel: +1415 397 0123
Email: cri-information@cryptography.com
Web: www.cryptography.com
Data security & cryptography

Cryptolog International
6-8 rue Basfroi
F-75011 Paris
France
Tel: +33 1 44 08 73 00
Email: sales@cryptolog.com
Web: www.cryptolog.com
Authentication Solutions & Cryptography

CTS Electronics
Corso Vercelli 332
10015 Ivrea
Italy
Tel: +39 0125 235 611
Email: direzione@ctsgroup.it
Web: www.ctselectronics.ctsgroup.it
ID Printing Equipment & Card Personalization

Cryptomathic A/S
Jægergårdsgade 118
DK-8000 Aarhus C
Denmark
Tel: +45 8676 2288
Web: www.cryptomathic.com
Manufacturing & Personalisation, smart card, access control

D

Datacard EMEIA
Forum 3,
Solent Business Park,
Whiteley,
Hampshire PO15 7FH
UK
Tel: +44 1489 555 600
Email: uksales@datacard.com
Web: www.datacard.com
Secure ID solutions, Manufacturing & Personalisation

Datacard Group is building on a 40-year heritage of innovation and customer success. Our portfolio of solutions, backed by expert service and support, enable card and secure ID programs for financial, government and other markets worldwide. With an unmatched commitment to customer satisfact ion, Datacard remains the industry's leading brand of secure ID and card personalization solutions.

Daon
11955 Freedom Drive
Suite 16000
Reston, VA 20190
USA
Email: info@daon.com
Web: www.daon.com
Biometric and Identity Solutions.

Datacon Technology GmbH
Datacon Headquarters,
Radfeld Innstr. 16
A-6240 Radfeld
Austria
Tel: +43 5337 600 0
Email: info.dceu@datacon.at
Web: www.datacon.at
RFID Solutions, Machinery

Datastrip Ltd
1 Thame Park Business Centre
Wenman Road
Thame, Oxfordshire
OX9 3XA
UK
Tel: +44 1844 215 668
Email: uk@datastrip.com
Web: www.datastrip.com
Secure ID solutions, Biometric solutions

De La Rue Identity Systems
De La Rue House
Jays Close Viables
Basingstoke,
Hampshire RG22 4BS
UK
Tel: +44 1256 605 000
Email: indentity.systems@uk.delarue.com
Web: www.delarue.com
Secure ID solutions, Holograms

Dedem Automatica Srl.
Via Cancelliera, 59
Roma

00040 - Ariccia
Italy
Tel: +39 06 930261
Email: info@dedem.it
Web: www.dedem.it
Personalisation: passports, drivers licenses and ID cards

DESKO GmbH
Gottlieb-Keim-Str. 56
Bayreuth
95448
Germany
Tel: +49 921 79279 0
Email: info@desko.de
Web: www.desko.de
Readers & Terminals, Access control

DigiCrypto Inc.
8 Corporate Park
Suite 300
Irvine
CA 92606
USA
Tel: + 1 949 981 9600
Email: info@digicrypto.com
Web: www.digicrypto.com
Card Personalisation , PKI solution provider

Digital Identification Solution
Teckstraße 52
Esslingen am,
Neckar 73734
Germany
Tel: +49 711 341689 0
Email: mail@digital-identification.com
Web: www.digital-identification.com
Manufacturing, & Personalisation, ID & Authentication, ID card & Security identification solutions

DILETTA ID Systems
Adam-Opel-Strasse 6
64569 Nauheim
Germany
Tel: +49 6152 1804 0
Email: contact@diletta.com
Web: www.diletta.com
personalisation systems and machine readable passports

DITTO Information Technology Inc.
Rm321 Daegu Techno Park venture plant,
711, Pasan-Dong,
Dalseo-gu,
Daegu 704-230
Korea
Tel: +82 53 325 5600
Email: ditto@dittotec.com
Web: www.gitc21.net/co/dittotec
Fingerprint Technology

Document Security Systems, Inc.
New York Address
28 Main Street East,
Suite 1525
Rochester,
NY 14614
USA
Tel: +1 585 325 3610
Web: www.documentsecurity.com
ID security solutions

E

EBV Elektronik
Im Technologiepark 2-8
Poing D-85586
Germany
Tel: +49 8121 7740
Web: www.ebv.com
Semiconductor manufacturer

Ecebs Ltd.,
The Torus Building
Rankine Avenue
Scottish Enterprise Technology Park
East Kilbride
Glasgow G75 0QF
UK
Tel: +44 (0) 1355 272911
Email: enquiries@ecebs.com
Web: www.ecebs.com
Ecebs Multefile smart card echnology, e -Passport, Healthcards and ID Authentication

EDAPS Consortium
64 Lenina Str.,
Kyiv 02088
Ukraine
Tel: +38 044 561 25 90
Email: edaps@edaps.ua
Web: www.edaps.ua
ID security documents, personalisation

EDSI
immeuble Atalis 1
1 rue de Paris
35510 Cesson-Sevigne,
France
Tel: +33 2 23 45 14 30
Web: www.edsi-smartcards.com
Manufacturing & Personalisation, Readers & Terminals, Access control, Card test tools,

Electronic Trade Solutions Ltd.
Beaux Lane House
Mercer Street Lower
Dublin 2
Ireland
Tel: +353 87 929 0768
Email: info@eKrypto.com
Web: www.ekrypto.com
Readers & Terminals, ID & Authentication, Access control

Electronics & Telecommunications Research Institute
138 Gajeongno
Yuseong-gu
Daejeon 305-700
Korea
Tel: +82 42 860 6114
Email: brcastle@etri.re.kr
Web: www.etri.re.kr
Biometric Solutions

Elliott Data Systems
Memphis, TN
5045 Covington Way
Memphis TN 38134
USA
Tel: +1901 372 4600
Email: identity@elliottdata.com
Web: www.elliottdata.com
Consulting, Card Personalisation, Solutions Provider

Emerging Technology Services Ltd
Suite 119
34 Buckingham Palace Road
London
SW1W 0RH
UK
Tel: +44 1604 660125
Email: mail@ets.uk.com
Web: www.ets.uk.com
Consultancy, biometrics and other identification technology

Entrust
One Lincoln Centre (directions)
5400 LBJ Freeway
Suite 1340
Dallas,
Texas 75240
USA
Tel: +1 888 690 2424

Email: entrust@entrust.com
Web: www.entrust.com
Identity-based security solutions, authentication, digital certificates, SSL & PKI

ExpoGraf Cardkeep International AB
Stillestorps Industriväg 1,
SE-443 61 Stenkullen,
Sweden
Tel: +46 (0)302 374 80
Email: info@cardkeep.se
Web: www.cardkeep.com
ID solutions

Exponent Inc.
149 Commonwealth Drive
Menlo Park
CA 94025
USA
Tel: +1 650 326 9400
Email: info@exponent.com
Web: www.exponent.com
Identification Devices

F

Fasver
286 rue Charles Gide
ZAE La Biste
BP48 34671 Baillargues Cedex
France
Tel: +33 4 67 87 66 99
Email: fasver@fasver.com
Web: www.fasver.com
Manufacturing & Personalisation

Feitian Technologies Co., Ltd.
Floor 17th, Tower B,
Huizhi Mansion, 9 Xueqing Road
Haidian District,
Beijing,100085
China
Tel: +(86)010-62304466
Fax: +(86)010-62304416
Email: world.sales@ftsafe.com
Web: www.FTSafe.com
Electronic ID Smart card manufacturer

FIME
Immeuble le Phénix 1
24 rue Émile Baudot
91120 Palaiseau
France
Tel: +33 (0) 1 64 53 36 50
Web: www.fime.com
ePassport testing

FQ Ingenieria Electronica
Polígono Industrial Vilanoveta,
Av. de les Roquetes, 9
08812 Sant Pere de Ribes
Barcelona
Spain
Tel: +34 932 08 02 58
Email: info@fqingenieria.es
Web: www.fqingenieria.es
Smart ID Systems: Terminals & RFID & Chips

Fujitsu Components Europe
Diamantlaan 25
2132 WV Hoofddorp
The Netherlands
Tel: +31 23 556 0910
Email: info@fceu.fujitsu.com
Web: www.emea.fujitsu.com
Printing & ID, Electronic Data Systems

G

Gemalto NV
Barbara Strozzilaan 382
1083 HN Amsterdam,
The Netherlands
Tel: +31 20 562 06 80
Web: www.gemalto.com
ID solutions

Get Group
El Boustan Street, Area 12
Sheraton - Heliopolis,
Cairo,
Egypt
Tel: +202 226 910 74
Email: hhonsy@getgroup.com
Web: www.getgroup.com
Manufacturing & Personalisation

For more than two decades, GET Group has led the Passport and ID industry with cutting edge systems utilizing Toppan printers - the world's most advanced secure document personalization equip ment, along with GET suite of proprietary software solutions. GET Group proudly presents the eP600, the newest generation of legendary high security passport personalization printers.

GET. Into the Future.

Ghirlanda Smart Card Solutions SPA
via Borgogna 2,
20122 Milan,
Italy
Tel: +39 02 972 33 1
Email: ghirlanda@ghirlanda.it
Web: www.ghirlanda.it
Manufacturing & Personalisation
Passport & ID solutions

GIE SESAM-Vitale
5, Boulevard Marie et Alexandre
Oyon, 72019 Le Mans Cedex 2
France
Tel: +33 811 709 710
Email: gie@sesam-vitale.fr
Web: www.sesam-vitale.fr
Systems integrator

Giesecke & Devrient

Giesecke & Devrient GmbH
Prinzregentenstrasse 159,
P.O. Box 80 07 29,
81607 Munich
Germany
Tel: +49 89 4119 0
Email: government@gi-de.com
Web: www.gi-de.com
ID cards and IT security (PKI)

The Giesecke & Devrient Group (G&D) is a leading global technology provider with its headquarters in Munich, Germany, and 65 subsidiaries, joint ventures, and associated companies across every continent.

Security, competence, and trust are the watchwords of the Group. Its customer-centric products, systems, and services make G&D a reliable partner for governments, central banks, high-security printers, public authorities, and other companies.

Global Enterprise Technologies GET Group
230 Third Ave, Waltham,

Waltham, MA 02451,
USA
Tel: +1 781890 6700
Email: info@getgroup.com
Web: www.getgroup.com
ID systems integrator, Passports & ID cards
issuing systems

Green Bit S.p.A.
Strada Antica di Grugliasco, 116
10095 Grugliasco (TO)
Italy
Tel: +39 011 7703811
Web: www.greenbit.com
Fingerprint Scanner & SmartCard and RFID reader/writer modules

Grid Sure Ltd.
Orchard House,
Heath Road,
Warboys,
Cambs. PE28 2UW,
UK
Tel: +44 1487 825 014
Web: www.gridsure.com
ID & Authentication

H

HID Global
15370 Barranca Pkwy
Irvine,
CA 92618-3106
USA
Tel: +1 949 732 2000
Email: info@hidglobal.com
Web: www.hidglobal.com.
Secure identity solutions

Hitachi ID Systems, Inc.
500, 1401 - 1st Street S.E.
Calgary,
Alberta T2G 2J3
Canada
Tel: +1.403 233 0740
Email: sales@Hitachi-ID.com
Web: www.hitachi-id.com
Identity and access management software/Hitachi ID Password Manager

HJP Consulting GmbH
Hauptstraße 35
33178 Borchen
Germany
Tel: +49 5251 41776 0
Email: info@hjp-consulting.com
Web: www.hjp-consulting.com
Manufacturing & Personalisation,
Smart card solutions: e-passports, eID cards & eHealth card

Hobim Data Processing Corp.
Cevreyolu Caddesi
2 - Bayrampasa
34030 Istanbul
Turkey
Tel: +90 212 467 24 67
Email: hobim@hobim.com
Web: www.hobim.com
Card Manufacturers & Suppliers of Holographic Cards

Hologram Industries
22, avenue de l'Europe
Bussy Saint Georges 77600
France
Tel: +33 1 64 76 31 00
Email: sales@hologram-industries.com
Web: www.hologram-industries.com
Manufacturing, & Personalisation,
Holograms

hw-engineering GmbH & Co. KG
Im Schönblick 24
DE - 73066 Uhingen
Germany
Tel: +49 7163 530818
Email: info@hw-eng.com
Web: www.hw-eng.com
Manufacturing, & Personalisation
ID & Authentication, Holograms,
Machinery: personalisation

Human Recognition Systems
1st Floor, Building 2000,
Vortex Court
Enterprise Way
Wavertree Technology Park
Liverpool L13 1FB
UK
Tel: +44 (0) 151 254 2888
Web: www.hrsltd.com
Secure Identity system integrator and consultancy, focused on biometric technology, identity management

I

IAI industrial systems bv
De Run 5406
5504 DE Veldhoven
P.O. Box 200
The Netherlands
Tel: +31 40 254 24 45
Email: info@iai.nl
Web: www.iai.nl
Personalisation systems, ID & Authentication, Passports

Icar
Ronda Can Fatjó, 21
Parc Tecnològic del Vallès
08290 Cerdanyola del Vallès
Spain
Tel: **+34) 935 942 474**
Email: icar@icarvision.com
Web: www.icarvision.net
Authentication of official documents of identity, facial recognition

ICC Solutions
St James Court
Warrington
Cheshire WA4 6PS
UK
Tel: +44 1925 629 001
Email: info@iccsolutions.com
Web: www.iccsolutions.com
Testing tools

ID Data Systems Ltd
The New Mint House
Bedford Road
Petersfield
Hants GU32 3AL
UK
Tel: +44 1730 235700
Email: freshthinking@iddata.com
Web: www.iddata.com
Card solutions provider

ID3 Semiconductors
5 rue de la Verrerie
38120 Fontanil-Cornillon
Rhône Alpes
France
Tel: +33 4 76 75 75 85
Email: contact@id3.eu
Web: www.id3.eu
Readers & Terminals, ID solutions

Identita Technologies Inc.
4580 Dufferin Street
Suite 500
North York,
Ontario, M3H 5Y2
Canada
Tel: +1 416-650-9505
Email: info@identita.com
Web: www.identita.com
Manufacturing & Personalisation
ID smartcards, Machinery: lamination

IDpendant GmbH
Edisonstr. 3
85716 Unterschleissheim
Germany
Tel: +49 89 3700110 0
Email: info@idpendant.com
Web: www.idpendant.de
Readers & Terminals

ID Technology Partners, Inc.
Conference and Technology Center
12 S. Summit Avenue
Suite 110
Gaithersburg,
MD 20877
USA
Tel: +1 301 990 9061
Email: info@idtp.com
Web: www.idtp.com
Identification and credentialing solutions

iDTRONIC GmbH
Donnersbergweg 1
67059 Ludwigshafen
Germany
Tel: +49 62 166900940
Email: info@idtronic.de
Web: www.idtronic-group.de
RFID Readers, RFID Tags

Impinj
701 N. 34th Street,
Suite 300
Seattle,
WA 98103
USA
Tel: +1 206 517 5300
Email: rfid_info@impinj.com
Web: www.impinj.com
RFID solutions, Readers & Terminals, Systems integration

Impuls France
30, Allée de Bretagne
ZI Nord 26300 Bourg de Peage
France
Tel: +33 4 75 71 08 50
Email: ifra@impulsid.com
Web: www.impulsid.com
Machinery: personalisation

Incard
Z.I. Marcianise Sud
1-81025 Marcianise (CE)
Italy
Tel: +39 0823 630 111
Email: info.incard@st.com
Web: www.incard.it
Manufacturing & Personalisation, Manufacturers smart cards, ID smartcards, Readers & Terminals,

Infineon Technologies France S.A.S
39/47, Boulevard Omano
93527 Saint-Denis CEDEX
France
Tel: +33 1 48097200
Web: www.infineon.com
Chip manufactuing, ePassport solutions

IMA s.r.o.
Institute of Microelectronic Applications
Na Valentince 1003/1,
150 00 Prague 5
Czech Republic
Tel: +420 2 5108 1097
Email: ima@ima.cz
Web: www.ima.cz
Single-chip microcomputers and identification cards

InkSure Inc.
551 Fifth Avenue
24th Floor
New York, NY 10176
Tel: +1 646 233 1454
Email: info@inksure.com
Web: www.inksure.com
Document security & authentication solutions

Innovative Card Technologies (InCard)
US Bank Tower
633 West 5th St. Suite 2600
Los Angeles
CA 90071
USA
Tel: +1 213 223 2145
Web: www.incard.com
ID & Authentication, Manufacturing & Personalisation, ID Management software, Access Control

Inteligensa
Rua Quintana, 887, 50. Andar,
Brooklin 04569-011
São Paulo
Brazil
Tel: +55 115105 4950
Web: www.inteligensa.com
Manufacturing, & Personalisation, ID & Authentication, ePassports,

Inspectron Ltd
Apex House
West End, Frome
Somerset BA11 3AS,
UK
Tel: +44 01373 452555
Email: info@inspectron.com
Web: www.inspectron.com
Document Verification solutions, ePassports

Intercede Group plc
Lutterworth Hall, St. Mary's Road
Lutterworth LE17 4PS
UK
Tel: +44 1455 558 111
Email: info@intercede.com
Web: www.intercede.com
Identity Credential Management

Interpolaris
1 North Bridge Rd,
06-22 High St. Centre
Singapore 179094
Singapore
Tel: +65 6338 8370
Email: info@interpolaris
Web: www.interpolaris.net
OEM technology distribution and consultancy for Government secure credentialing processing

Iris ID Systems, Inc.
7 Clarke Drive,
Cranbury,
NJ 08512,
USA
Tel: +1 609 819 4747
Web: www.irisid.com
Iris identity authentication technologies, IrisAccess platform

Intercede Group plc
Lutterworth Hall, St. Mary's Road
Lutterworth,
Leicestershire LE17 4PS
UK
Tel:. +44 1455 558 111
Email: info@intercede.com
Web: www.intercede.com
MyID identity and credential management system

Isolane/Eurintel
8, Boulevard Détriché
49000 ANGERS
France
Tel: +33 2 41 88 66 18

Email: contact.isolane@eolane.com
Web: www.isolane.com
Designs & Manufactures Card Personalisation systems

IXLA S.A.
Otierdo 32
CH 1754 Avry
Switzerland
Email: info@ixla.ch
Web: www.ixla.ch
ID-cards & e-Passport personalisation

J

Jaypeetex Engineering
231, Udyog Bhavan
Sonawala Road
Goregaon (East)
Mumbai 400 063
India
Tel: +91 22 2686 5421
Email: info@jaypeetex.com
Web: www.jaypeetex.com
Biometrics Technology, Fingerprint Readers

JDS Uniphase Corporation
430 N. McCarthy Blvd.
Milpitas,
CA 95035
USA
Tel: +1 408 546 5000
Web: www.jdsu.com
Document security & authentication solutions

K

Kare Corporation
7, 2nd Link Street, CIT Colony
Mylapore
Chennai - 600 004
Tamilnadu
India
Tel: +91 44 39 123 123
Email: info@karecorp.com
Web: www.karecorp.com
identification system & card manufacturer: Smart Card Solutions, Personalisation Systems & Biometrics

KBA Metronic Aktiengesellschaft
Benzstraße 11
97209 Veitshöchheim
Germany
Tel: +49 931 9085 0
Email: info@kba-metronic.com
Web: www.kba-metronic.com
Machinery: personalisation

Keesing Reference Systems
P.O. Box 12476
1100 AL AMSTERDAM
The Netherlands
Tel: +31 (0)20 7157800
Email: info@keesingfightfraud.com
Web: www.keesingfightfraud.com
Verification tools and solutions / authenticate ID documents

koera-packmat
Gewerbestrafle 4
D-78667 Villingendorf
Germany
Tel: +49 741 9283-0
Email: info@koera-packmat.de
Web: www.koera-packmat.de
Card Personalization and Wrapping Systems

KSW Microtec AG
Manfred-von-Ardenne-Ring 12
D-01099 Dresden
Germany
Tel: +49 351 88960-10
Email: office@ksw-microtec.de
Web: www.ksw-microtec.de
RFID components for logistics and public transport, contactless credit cards and access systems

KURZ
Schwabacher Straße 482
90763 Fuerth
Germany
Tel: +49 911 71 41 0
Email: sales@kurz.de
Web: www.kurz.de
Card Manufacturer & card personalisation

KURZ is a major international supplier of hot stamping technology. KURZ hot stamping foils are utilized on a wide assortment of products. These include packaging, greeting cards, electronic devices, household appliances, cosmetics, textiles, furniture, automotive parts, and numerous other items. KURZ's state-of-the-art application technology, magnetic foils, and holograms provide effective and attractive brand name protection, as well as increased security for businesses everywhere.

L

L-1 Identity Solutions Secure Credentialing Division
296 Concord Rd.
Billerica,
MA 01821
USA
Tel: +1 1 978 215 2400
Email: SCDinfo@l1id.com
Web: www.l1id.com/securecredentialing
Identity management solutions

L-1 provides complete identity management solutions that form the foundation for the most secure credentials used today. L-1 produces millions of secure government-issued IDs worldwide each year, including driver's licenses, National IDs, Voter Registration Cards, and passports, ensuring that travelers are who they claim to be and protecting the world against crime perpetrated by fraudulent identities.

LAB ID srl
Via Corticella 11/4
40013 Castel Maggiore (BO)
Loc. Trebbo di Reno ,
Italy
Tel: +39 051 70 59 41
Email: info@lab-id.com
Web: www.lab-id.com
RFID technology for identification

Landqart AG
Kantonsstrasse 16
CH-7302 Landquart
Switzerland
Tel: +41(0)81 307 90 90
Web: www.landqart.ch
Document security solutions / Security Paper & Identity papers

LaserCard Corporation
Global Corporate Headquarters
1875 N. Shoreline Blvd.
Mountain View,
CA 94043
USA
Tel: +1 650 969 4428
Email: sales@lasercard.com
Web: www.lasercard.com
ID credential solutions: national ID, foreign resident; worker ID, drivers' licenses, student ID, e-passports, Access control

LEGIC Identsystems Ltd.
Binzackerstrasse 41
Post Box 1221
CH-8620 Wetzikon Zurich
Switzerland
Tel: +41 44 933 64 64
Email: info@legic.com
Web: www.legic.com
Manufacturing smartcards, Readers & Terminals, Access control

LEGIC Identsystems Ltd, leading supplier of 13.56 MHz contactless smart card technology offers highly integrated LEGIC RF Standard, ISO15693 /ISO14443 compliant read and write security modules, transponder chips and advanced NFC solutions (member of the NFC Forum). The LEGIC all-in-one card tech nology, specially designed for physical access and related multi applications, is used for company cards, ticketing and leisure passes across all industry sectors such as aerospace, banking, public services, universities, government, airports and leisure/ recreational areas.

Facts:
- Over 200 partners worldwide
- 2 million readers
- 100 million credentials
- More than 60,000 business and leisure installations around the world

LEONHARD KURZ Stiftung & CO. KG
Schwabacher Straße. 482
D-90763 Fuerth
Germany
Tel: +49 911 71 41-0
Email: guenther.friedl@kurtz.de
Web: www.kurz.de
Manufacturer & Personalisation
KURZ-signature foils & holograms

Lumidigm, Inc.
801 University Blvd SE, Ste 302
Albuquerque,
NM 87106
USA
Tel: +1 505 272 7084
Web: www.lumidigm.com
Biometric identification and verification, fingerprint sensor

LUX Ident s.r.o.
Tovární 368
CZ-56301 Lanskroun
Czech Republic
Tel: +420 465 352 500
Email: info@lux-ident.com
Web: www.lux-ident.com
Manufacturing & Personalisation
ID & Authentication, Smart cards & Smart Labels

M

Magicard
Ultra Electronics Card Systems Inc.
6711 - 176th Avenue NE,
Redmond,
Washington, 98052,
USA
Tel: +1 425 556 9708
Email: americas@magicard.com
Web: www.ultramagicard.com
Printers used for ID, membership, access control, and loyalty applications

MagTek Inc.
1710 Apollo Court,
Seal Beach,
CA 90740
USA
Tel: +1 562 546 6400
Web: www.magtek.com
Card Personalisation & Issuance

MaskTech GmbH
Nordostpark 16
90411 Nuremberg
Germany
Tel: +49 911 955149 0
Email: support@masktech.de
Web: www.masktech.de
Card Personalisation & Card mailing systems

Matica System
7th Floor Phoenix House
18th King William Street
London, EC4N 7HE
UK
Tel: +39 051 671 331
Email: sales@maticasystem.com
Web: www.maticasystem.com
Card Personalisation Systems

MaxID Corp
2371-C Prosperity Avenue
Fairfax, VA 22031
USA
Tel: +1 925-468-0109
Email: info@maxid.net
Web: www.maxid.net
Identity and security solutions, biometric handheld devices

Maze Cards
A-242, T T C Industrial Area,
Near Mahape Bus Depot Navi
Mumbai 400 701
India
Tel: +91 22 2778 0430
Email: info@mazecards.com
Web: www.mazecards.com
RFID to Chip/ID Solutions, personalistion

Merkatum Corp.
Braker Pointe
10801-2 N. MoPac Expressway,
Suite 230
Austin, Texas 78759
USA
Tel: +1.512 687 3157
Email: contactusa@merkatum.com
Web: www.merkatum.com
Biometric and biographic identity resolution systems

Metaform
1 Hanagar St.
P.O.B. 7252
Neve Ne'eman
Hod Hasharon, 45241
Israel
Tel: +972 3 53 120 20
Email: sales@metaform.co.il
Web: www.metaform-ltd.com
Identification Solutions & Document Issuance Management

Mediscs
Espace Concorde
Parc d'Activités Aéroport
120 Impasse Jean Baptiste SAY
34470 Pérols
France
Tel: +33 4 99 63 68 30
Email: info@mediscs.com
Web: www.mediscs.com
ID & Authentication, e-authentication

MELZER maschinenbau GmbH
Ruhrstr. 51-55
58332 Schwelm
Germany
Tel: +49 2336 9292 0
Email: sales@melzergmbh.com
Web: www.melzermaschinenbau.de
Manufacturing: machines, tags and labels, e-passports, e-passport visa, RFID tickets,

MIOS SAS
Bâtiment B Tech'Indus
645, rue Mayor de Montricher
Pôle d'activités d'Aix-les-Milles
BP 50 108
13793 Aix en Provence Cedex 3
France
Tel: +33 442 24 32 40
Fax: +33 442 39 78 36
Email: contact@mios.fr
Web: www.mios.fr
Secure access control

SAFRAN
Morpho

Morpho
Formerly Sagem Identification
Oudeweg 32,
2031 CC Haarlem,
The Netherlands
Tel: +31 23 799 5514
Fax: +31 23 799 5180
Email: info@morpho.com
Web: www.morpho.com
Biometric, Identification smart systems

Morpho, a high-technology company in the Safran group, is one of the world's leading suppliers of identification, detection and e-document solutions. Morpho is specialized in personal rights and flow management applications based on biometrics, secure terminals and smart documents. Morpho's integrated systems and equipment are deployed worldwide and contribute to the safety and security of transportation, data, people and countries.

Morpho e-Documents
former Sagem Orga GmbH
Riemekestr. 160
33106 Paderborn
Germany
Tel: +49 (0) 5251 889 0
Email: info@sagem-orga.com
Web: www.morpho-edocs.com
ID-cards, ePassports solutions

Mühlbauer
High Tech International

Mühlbauer AG
Josef-Mühlbauer-Platz 1
93426 Roding
Germany
Tel: +49 9461 952 0
Email: info@muehlbauer.de
Web: www.muehlbauer.de
ID-cards, ePassports, e-driving licences, e-NID cards and RFID labels, ID card solutions

The Mühlbauer Group is a premium partner for private companies and the public sector in the areas of smart ID solutions and RFID applications. Our unique portfolio and a complete technology and know-how transfer make us the preferred technology partner for governments, security printers and system integrators. Trust in the ID solutions specialist – trust in Mühlbauer.

N
nagra ID

Nagra ID SA - Kudelski Group
Crêt-Du-Locle 10,
P.O. Box 1419 2301
2301 La Chaux-de-Fonds,
Switzerland
Tel: +41 32 924 04 04
Fax: +41 32 924 0400
Email: info@nagraid.com
Web: www.nagraid.com
Contact for Government solutions:
Government@nagraid.com
Secure ID solutions, Manufacturing & Personalisation

NagraID offers tailor-made solutions based in multi-application smart card solutions including high security printing features with contact and/or secure contactless technology, and has developed a unique and patented process to manufacture ISO Display Cards for citizens ID's and secure ID's use applications.

We support also Citizens ID programs with our NagraID Bio-platform that is an ideal solution for rapidly and safely deploying applications such as national e-ID's, eHealth and other ID programs. The core software of our Bio-platform solution are based in the latest technologies available on the market (COTS - Commercial-Off The-Shelf) and has been designed and integrated transparently with other information and business systems. This approach insures that the system provided has robust and scalable foundations that comply with current national and international standards.

Secure Manufacturing Plant for ID Credentials certified ISO 9001:2000

Established in 1976, NagraID joined the Kudelski Group in 2001. Our headquarters are located in La Chaux-de-Fonds (Switzerland), the cradle of the world's watchmaking industry.

SWISS COMPETENCE IN IDENTIFICATION

Narboni
3, Avenue d'Amazonie
ZA de Courtaboeuf
91952 Les Ulis cedex
France
Tel: + 33 1 60 92 65 42
Email: contact@narboni.com
Web: www.narboni.com
Manufacturer & Personalisation

NBS Technologies
703 Evans Avenue,

Suite 402
Toronto,
Ontario M9C 5E9
Canada
Tel: +1 416.621.1911
Fax: +1 416.621.8875
Web: www.nbstech.com
Card personalization, ID cards, ID card printing

NEC Corporation
7-1, Shiba 5-chome
Minato-ku
Tokyo 108-8001
Japan
Tel: +81 3 3454 1111
Web: www.nec.co.jp
Biometrics/Security ID System Solutions

NEOWAVE
1480, avenue d'Arménie
13120 Gardanne
France
Tel: +33 (0)4 42 50 70 05
Email: contact@neowave.fr
Web: www.neowave.fr
NFC IDentity solution

Nimax Plastic Card Division
via dell'Arcoveggio 59/2
40129 Bologna
Italy
Tel: +39 051 419 9111
Email: card_division@nimax.it
Web: www.nimaxcard.com
Card Production Equipment, Card Personalisation

NTX Research SA
111 avenue Victor Hugo
75116 Paris,
France
Tel: +33 (0)1 47 66 39 85
Email: ntx(at)ntx-research.com
Web: www.ntx-research.com
XC cryptographic technology & authentication for mobile phone, smartphone, smartcard.

NXP
4 rue du port aux Vins
92150 Suresnes
France
Tel:+33 (0)1 40 99 52 00
Web: www.nxp.com
IC provider for electronic ID documents

Oberthur Technologies
50, quai Michelet
92352 Levallois-Perret
France
Tel: +33 1 55 46 71 34
Email: info@oberthur.com
Web: www.oberthurcs.com
Manufacturing, & Personalisation ID smart cards

Oberthur is one of the world leaders in the field of secure technologies.
- Smart cards: One of the world's leading providers of security and identification based on smart card technology and associated services, such as personalization, for the mobile, payment, identity markets.
- Secure printing: 3rd private security printer, specializing in high security for the production and management of banknotes, passports and other identity documents
- Cash protection: World leader in equipments for smart cash transportation and ATM protection.
Listed on Euronext Paris, Oberthur benefits from an industrial and worldwide commercial presence.

OmniPerception Ltd
20 Nugent Road,
Surrey Research Park
Guildford,
Surrey GU2 7AF
UK
Tel: +44 (0)1483 688350
Email: info@omniperception.com
Web: www.omniperception.com
Identity management solutions with in-built facial biometrics

OPSEC Security Ltd
40 Phoenix Road
Crowther Industrial Estate
Washington,
Tyne & Wear NE38 OAD
UK
Tel: +44 191 417 5434
Email: info@opsecsecurity.com
Web: www.opsecsecurity.com
ID Security Solutions: passports, secure identity card solutions

Optaglio Ltd.,
Basepoint Business Centre
Caxton Close
East Portway Industrial Estate
Andover
Hants SP10 3FG,
UK
Tel: +44 (0) 1264 336 510
Email: info@optaglio.com
Web: www.optaglio.com/en/main
ID solutions, Data protection laminates and thin overlays

On Track Innovations, Ltd. (OTI)
ZHR Industrial Zone
P.O. Box 32
Rosh Pina, 12000
Israel
Tel: +972 4 6868000
Email: info@otiglobal.com
Web: www.otiglobal.com
Manufacturing & Personalisation ID & Authentication, Machinery:Smart OID solutions, card ePasspots

Otto Künnecke GmbH
Zeppelinstrasse 10
37603 Holzminden
Germany
Tel: +49 (0) 55 31 / 9300 - 0
Email: contact@kuennecke.com
Web: www.kuennecke.com
Personalisation security solutions: passports, ID-and bank-cards

Orcanthus
18, rue de Cosswiller,
67310 Wasselonne
Alsace,
France
Tel: +33 3 88 40 25 01
Web: www.orcanthus.com
Access control, Biometrics, RFID solutions

ORIBI Software
Bedrijfsweg 15
5061 JX Oisterwijk
The Netherlands
Tel: + 1 (0)13 52 11 256
Email: info@oribi.nl
Web: www.oribi.nl
ID-Management solutions: verify identity documents,

OVD Kinegram AG
Zählerweg 12
CH-6301 Zug
Switzerland
Tel: +41 41 724 47 00
Web: www.kinegram.com
Manufacturer of Optical Security solutions, Hot embossing film. Goverment documents.

P

Paragon Identification
Les Aubepins
18410 Argent-sur-Sauldre
France
Tel: +33 2 48 81 61 00
Email: identification@ identification.fr
Web: www.paragon-identification.fr
Personalisation Systems

PAV
Hamburger Strasse 6
D-22952 Lütjensee
Germany
Tel: +49 4154 799 0
Email: info@pav.de
Web: www.pav.de

Smart Cards, Contactless cards with different chip types, PET and PC cards, Memory and processor chip cards, Customer loyalty cards, Gift cards, Card personalization, passport inlays, Card prelaminates

PAV is a well-established company with a rich tradition and employs around 250 staff members. Our long experience and high-end technology allows us to offer a wide range of smart cards designed for identification purposes including personalization.
Also, PAV provides companies in developing and producing their first samples. To maintain our edge for innovation, PAV has its own R&D department. Here we realised the development of ICAO compliant electronic inlays for biometric passports. Our ePassport inlays made from polycarbonate or synthetic paper are suited for further processing in every standard passport production.
For all activities we go for a retentive use of the resource to save the environment.

Payne Security
Wildmere Road
Banbury
OXON OX16 3JU
UK
Tel: +44 1295 265601
Email: info@payne-security.com
Web: www.payne-security.com
Personalisation system, ID & Authentication

Plastic-ID.com
2 Redhouse Square, Duncan Close,
Moulton Park,
Northampton, NN3 6WL
UK
Tel: +44 (0)844 736 1563
Email: info@plastic-id.com
Web: www.plastic-id.com
Plastic card printers, consumables and information & Pac Smart Card - Mifare

Precise Biometrics AB
Box 798
220 07 Lund
Sweden
Tel: + 46 46 31 11 00
Email: info@precisebiometrics.com
Web: www.precisebiometrics.com
Biometric solutions, Manufacturing & Personalisation, Card test tools

Prooftag SAS
1100, Avenue de l'Europe
F-82 000 MONTAUBAN
France
Tel: +33 5 63 21 10 50
Email: prooftag@prooftag.com
Web: www.prooftag.net
ID & Authentication

R

Regula Ltd
P.O. Box 39
Minsk 220036
Republic of Belarus
Tel: +375 17 2862825
Email: mail@regula.by
Web: www.regula.ws
ID security solutions, Readers & Terminals, passport readers, finger/palm print scanners

Renesas Technology Europe Ltd.,
Dukes Meadow,
Millboard Road
Bourne End
Bucks SL8 5FH
UK
Tel: +44 1628 585 100
Email: contact.eu@renesas.com
Web: www.renesas.eu
Chip manufactures
333 -1641 Lonsdale Ave., North Vancouver, British Columbia

ruhlamat GmbH
Sonnenacker 2,
99819 Marksuhl
Germany
Tel: +49 36925 929 0
Email: info@ruhlamat.de
Web: www.ruhlamat.de
Card personalisation

ruhlamat is an innovative German machine manufacturer providing equipment for the production of:

- Smart cards
- (e)-Passports
- RFID Inlays
- Chip modules

With an extensive background as an innovator in the industry, ruhlamat's particular areas of expertise in card personalisation are high quality laser engraving and HD DOD inkjet printing unmatched in today's industry.

S

Safe ID Solutions AG
Ottobrunner Straße 43
Unterhaching,
Bavaria 82008
Germany
Tel: +49 89 45 21 26 0
Email: info@safe-id.solutions.com
Web: www.safe-id.de
ID & Authentication

Safelayer Secure Communications, S.A.
Edificio Valrealty
C/ Basauri 17 Edif. B,
Plta. Baja Izq. Ofic. B
28023 Madrid
Spain
Tel: +34 917 080 480
Email: sflyr@safelayer.com
Web: www.safelayer.com
PKI (Public Key Infrastructure) for digital identification, electronic signature and data encryption for documents

SafeNet Inc.
4690 Millennium Drive
Belcamp,
MD 21017
USA
Tel: +1 410 931 7500
Email: orders@safenet-inc.com
Web: www.safenet-inc.com
ID & Authentication, smartcard security solutions

Scenecheck Europe BV
2621 Corrinado Court
Fort Wayne,
IN 46808
USA
Tel: +1 866 484 0611 0
Email: cfw.sales@screencheckna.com
Web: www.screencheckna.com
ID card systems, management solutions, ID card printers

SCM Microsystems GmbH
Oskar-Messter-Str. 13
85737 Ismaning,
Germany
Tel: + 49 89 9595 5000
Email: sales@scmmicro.de
Web: www.scmmicro.com
ID cards & passport readers & scanners

Scsquare
2A Harbarzel St.
Ramat Hahayal
Tel Aviv 69710
Israel
Tel: +972 3 765 7331
Email: marketing@scsquare.com
Web: www.scsquare.com
Personalisation Software & Authentication Solutions, ID card solutions

secunet Security Networks AG
Kronprinzenstr. 30
45128 Essen
Germany
Tel: +49 (0) 201 5454-0
Email: info@secunet.com
Web: www.secunet.com
Biometrics and Electronic ID Documents

Secure Tech
2013, East Mezzanine
Floor, Hajvairy Mansion,
Jinnah Avenue, Blue Area,
Islamabad
Pakistan
Tel: +92 51 2826346 7
Email: info@securetech-consultancy.com
Web: www.securetech-consultancy.com
Consultancy, ID Management secure solutions

Serverside Group Ltd.,
16 Kingly Street
London W1B 5PT
UK
Tel: + 44 20 7534 3833
Email: simon.drinkall@ssgl.com
Web: www.serversidegroup.com
Digital card design & Personalisation ID solutions

Shenzhen Theory Technology Co., Ltd.
2FL,1st Bullding,
Minqi Technology Park,
Pingshan, Xili,
Nanshan District,
Shenzhen 518055,
China
Tel: +86 755 2699 7700
Email: info@theory.com.cn
Web: www.theory.com.cn
ID smartcards, Access control,

Smart Packaging Solutions
Avenue Olivier Perroy
ZI de Rousset
13106 Rousset Cedex
France
Tel: +33 4 42 53 84 40
Email: contact@s-p-s.com
Web: www.s-p-s.com
Smart Packaging Solutions for e-passport, & bio-components, contactless inlays

Smart Packaging Solutions (SPS)
Avenue Olivier Perroy
ZI de Rousset
13106 Rousset Cedex
France
Tel: +33 4 42 53 84 40
Email: contact@s-p-s.com
Web: www.s-p-s.com
Manufacturing & Personalisation ID Solutions, ePassports

Smartdisplayer Technology
20F-8, No. 77, sec. 1,
Hsin-Tai-Wu Road,
Hsi-Chih,
Taipei County
Taiwan
Tel: +886 2 8698 2008
Email: service@smartdisplayer.com.tw
Web: www.smartdisplayer.com
ID smartcard

Smartmatic
1001 Broken Sound Parkway,
Suite D.
Boca Raton
FL 33487,
USA
Tel: +1 561 8620747
Email: usa@smartmatic.com
Web: www.smartmatic.com
Identity Management Solutions, Biometric security

Smartmetric
Hughes Center
Las Vegas,
Nevada 89109
USA
Tel: +1 702 799 9057
Web: www.smartmetric.com
Biometric cards, identity & transaction card

SMARTRAC N.V.,
Strawinskylaan 851
1077 XX Amsterdam
The Netherlands
Tel:+31 20 30 50 150
Email: info@smartrac-group.com
Web: www.smartrac-group.com
RFID systems for contactless data transmission

Smartware
11 avenue des Andes
"Le Carthagéne"
Z.A. de Courtaboeuf

91940 Les Ulis
France
Tel: +33 1 6486 2525
Email: contact@smartware.fr
Web: www.smartware.fr
Manufacturing & Personalisation, Card test tools, Readers & Terminals ID management solutions, TurnKey Solutions

SOGEDEX
Parc d'activités de Pissaloup
4, rue Edouard Branly
CS 30502
78197 Trappes Cedex
France
Tel: +33 1 30 68 66 00
Email: sogedex@sogedex.fr
Web: www.sogedex.com
Manufacturing & Personalisation ID & Authentication, ID solutions & software

Speed Identity AB
P.O. Box 634
S-135 26 Tyresö
Mediavogen 11
Sweden
Tel: +46 8 448 70 00
Web: www.speed-identity.com
Biometric Enrolment Solutions for Identity, ID card solutions

Springcard
13 voie la Cardon
Parc Gutenberg
91120 Palaiseau
FRANCE
Tel: +33 0 164 53 20 10
Email: info@springcard.com
Web: www.springcard.com
Readers & Terminals, Biometric & Contactless solutions

ST Incard S.r.l
Z.I. Marcianise Sud
81025 Marcianise (CE)
Marcianise
CE 81025
Italy
Tel: +39 0823 630 111
Email: info.incard@st.com
Web: www.incard.com
Manufacturers smart cards, Payment solutions

STMicroelectronics
39, Chemin du Champ des Filles
C. P. 21
CH 1228 Plan-Les-Ouates
Geneva,
Switzerland
Tel: +41 22 929 29 29
Web: www.st.com
Semiconductors manufacturer, Readers & Terminals, ID & Authentication

Sybernautix
1000 Great West Road
Brentford TW8 9HH
UK
Tel: +44 20 8263 5680
Email: info@sybernautix.com
Web: www.sybernautix.com
Consulting, Biometric security software solutions

T

TSSI Systems Ltd.,
Rutland House,
Hargreaves Road,
Groundwell Ind. Estate,
Swindon, SN25 5AZ
UK
Tel: + 44 1793 747700
Web: www.tssi.co.uk
Document & ID card security

Team Nisca
100 Randolph Road
Somerset,
NJ 08873
USA
Tel: +1 732 271 7367
Email: sales@teamnisca.com
Web: www.teamnisca.com
Machinery personalisaton, Machinery card printing

Teraco Inc.
2080 Commerce Drive
Midland
TX 79703
USA
Tel: +1 800 687 3999
Email: info@teraco.com
Web: www.Teraco.com
Personalisation & ID Cards, Plastic Cards

Thales
Security Solutions & Services Division
45 Rue De Villiers Cedex
Neuilly-sur-Seine 92200
France
Tel: +33 1 57 77 89 02
Web: www.thalesgroup.com
Readers & Terminals, Security & Identity systems

Thames Card Technology Ltd
Arterial Road
Rayleigh
Essex SS6 7UQ.
UK
Tel: +44 1268 775555
Email: info@thamesgroup.co.uk
Web: www.thamesgroup.co.uk
Plastic Card Manufacturer, Card Personalisation

Tiempo
110 rue Blaise Pascal
Bâtiment Viseo – Inovallée
38330 Montbonnot Saint Martin
France
Tel: +33 4 76 61 10 00
Email: web-contact@tiempo-ic.com
Web: www.tiempo-ic.com
Cryptoprocessors for embedded or high-level security applications such as contactless cards

TSSI Systems Ltd.
Rutland House, Hargreaves Road,
Groundwell Ind. Estate,
Swindon, SN25 5AZ,
UK
Tel: + 44 1793 747700
Email: support@tssi.co.uk
Web: www.tssi.co.uk
Manufacturer of biometric security and document security products and passport readers.

Todos Data System AB
Fiskhamnsgatan 2
SE-414 58 Göteborg,
Sweden
Tel: +46 31 775 8800
Email: info@todos.se
Web: www.todos.se
ID & Authentication, Authentication Solutions, Readers & Terminals

Toppan Printing Company
1 Kanda Izumi-cho Chiyoda-ku
Tokyo 101-0024
Japan
Tel: +81 3 3835 511
Web: www.toppan.com
ID & Authentication solutions

Trüb Group
Hintere Bahnhofstrasse 12
CH-5001 Aarau
Switzerland
Tel: +41 62 832 00 00
Email: info@trueb.ch
Web: www.trueb.ch
ID Card Solutions, Manufacturing & Personalisation, ID smartcards

Trüb is a leader, both in Switzerland and internationally, in secure and high quality identification solutions. Founded in 1859, the company is among the world's leading suppliers of national identity documents such as identity cards, driving licences and data pages for passports, as well as banking and customer loyalty cards and solutions for logical and physical access.
Over 30 countries on four continents – including Switzerland, UK, Czech Republic, Croatia, Poland, Estonia, Hong Kong and South Africa, are among the company's governmental clientele. Customers in the finance sector include in Switzerland UBS, Cornèr Bank, the entirety of Switzerland's cantonal banks and more than 40 other financial institutions in 20 countries.
The Trüb Group comprises a number of companies in Europe. In 2009 it generated a turnover of around CHF 151 million, and employs a staff of 445, including 305 in Switzerland.

U

Upek, Inc.
5900 Christie Ave.
Emeryville,
CA 94608
USA
Tel: +1 510 420 2600
Email: steve.hahm@upek.com
Web: www.upek.com
ID & Authentication, Biometrics and embedded RSA SecurID technology solutions

Utimaco Safeware
Ash House
Fairfield Avenue
Staines
Middlesex TW18 4AB
UK
Tel: +44 1784 22 42 25
Web: www.utimaco.co.uk
Experts on Data Encryption

V

Vasco Data Security NV/SA
Koningin Astridlaan 164,
Wemmel, B-1780
Belgium
Tel: +32 2 609 97 00
Email: info_europe@vasco.com
Web: www.vasco.com
ID & Authentication

Versatile Card Technology, Inc.
5200 Thatcher Road,
Downers Grove,
Illinois 60515
USA
Tel: +1 630 852 5600
Web: www.vct.com
Manufacturing & Personalisation, ID smartcards

Vlatacom d.o.o.
7 Dunavska St.
11080 Belgrade,
Serbia
Tel: +381 11 377 11 00
Email: info@vlatacom.com
Web: www.vlatacom.com
Personalisation: ID card and passport,

vps ID Systeme GmbH
Carl-Zeiss-Straße 2
76275 Ettlingen
Germany
Tel: +49 7243 5488 0
Email: info@vps.de
Web: www.vps.de
ID & Authentication, Personalisation

VTT GmbH
Auf dem Kessellande 2,
Niedersachsen
30900 Wedemark,
Germany
Tel: +49 5130 92 84 0
Email: info@vtt.de
Web: www.vtt.de
Personalisation Solutions
Machinery laminating, ePassports, ID smartcards, Driving Licence

W

Wacom Signature
Europark Fichtenhain A9
D-47807 Krefeld
Germany
Tel: +49-(0)2151-36 14-0
Email: info@wacom-europe.com
Web: www.signature.wacom.eu
Identity documents, signature solutions

Watchdata System Co. Ltd.
2 Yandong Business Park,
Wanhong West St. Capital Airport Rd.
Chaoyang District,
Beijing 100015
China
Tel: +86 10 6472 2288
Web: www.watchdata.com.cn
Smart card security systems

WINTER AG
Edisonstr. 3,
Unterschleißheim, Munich,
Bavaria, 85716,
Germany
Tel: +49 89 33034 0
Email: info@winter-ag.de
Web: www.winter-ag.de
ID & Authentication, ID smartcards

X

Xiring
River Seine, 25 Quai Galliéni
92158 Suresnes Cedex
France
Tel: +33 1 46 25 80 80
Email: contact@xiring.com
Web: www.xiring.com
ID & Authentication, e-ID

Z

Zetes
Da Vinci Science Park
Rue de Strasbourg 3
Straatsburgstraat 3
1130 Brussel
Belgium
Tel: +32 2 72837 11
Email: info@be.zetes.com
Web: www.zetes.com
ID Solutions

5th Edition

THE GLOBAL HUB FOR NEXT GENERATION CITIZEN & GOVERNMENT ID SOLUTIONS

SDW 2011

QUEEN ELIZABETH II CONFERENCE CENTRE, LONDON

CONFERENCE: 4–6 APRIL 2011 | EXHIBITION: 5–6 APRIL 2011

- Security documents, ePassports, advanced eID technologies, intelligent border control, document anti-counterfeiting...
- Fully international event with 70+ leading companies exhibiting from across the world
- Register to attend the exhibition for free, or book now for preferential conference rates
- Government Alert! Incredibly low conference rates available, plus buy one get second half price
- A limited number of free conference passes for African, Asian and Middle Eastern government attendees

If Government and Citizen ID markets are your business, SDW 2011 has the answers...

www.sdw2011.com

Organised by:
science media partners

Introducing ExianSmart; the First Contactless Card with a 15-Year Life

ExianSmart includes these features:

- Supports multiple modes of secure personalization including color and laser engraving
- Personalization done while assembling the card (no card blanks exist)
- Tamper-evident fused card
- RFID technology agnostic
- Range of chip memory sizes and operating systems
- ISO/IEC 14443 contactless smart card
- Chemical resistant
- EAL4+ security
- Meets ICAO 9303 National ID and ISO 18013 driver's license standards

www.L1ID.com/securecredentialing

L-1 IDENTITY SOLUTIONS™

SECURE CREDENTIALING DIVISION

The ExianSmart card is another example of L-1's innovation and leadership in providing the world with the most secure identity documents.